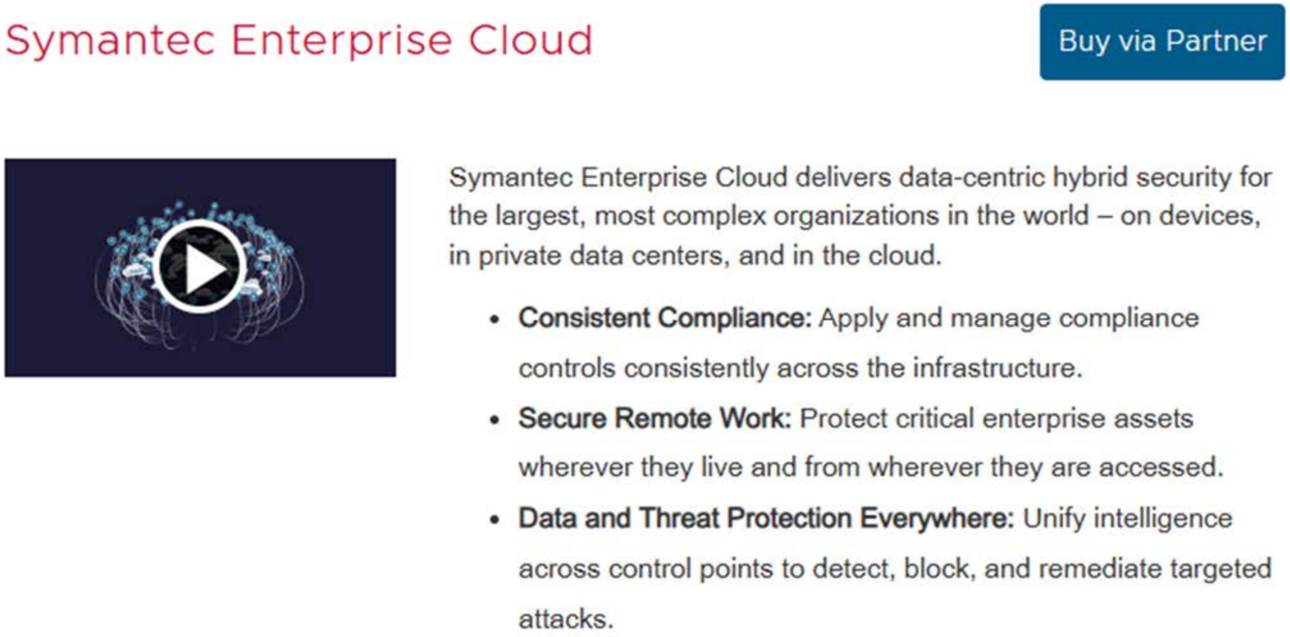
UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

QUICKVAULT, INC., Plaintiff, v. BROADCOM INC., d/b/a BROADCOM CORPORATION Defendant.	Case No.: 1:24-cv-00864 **JURY TRIAL DEMANDED**

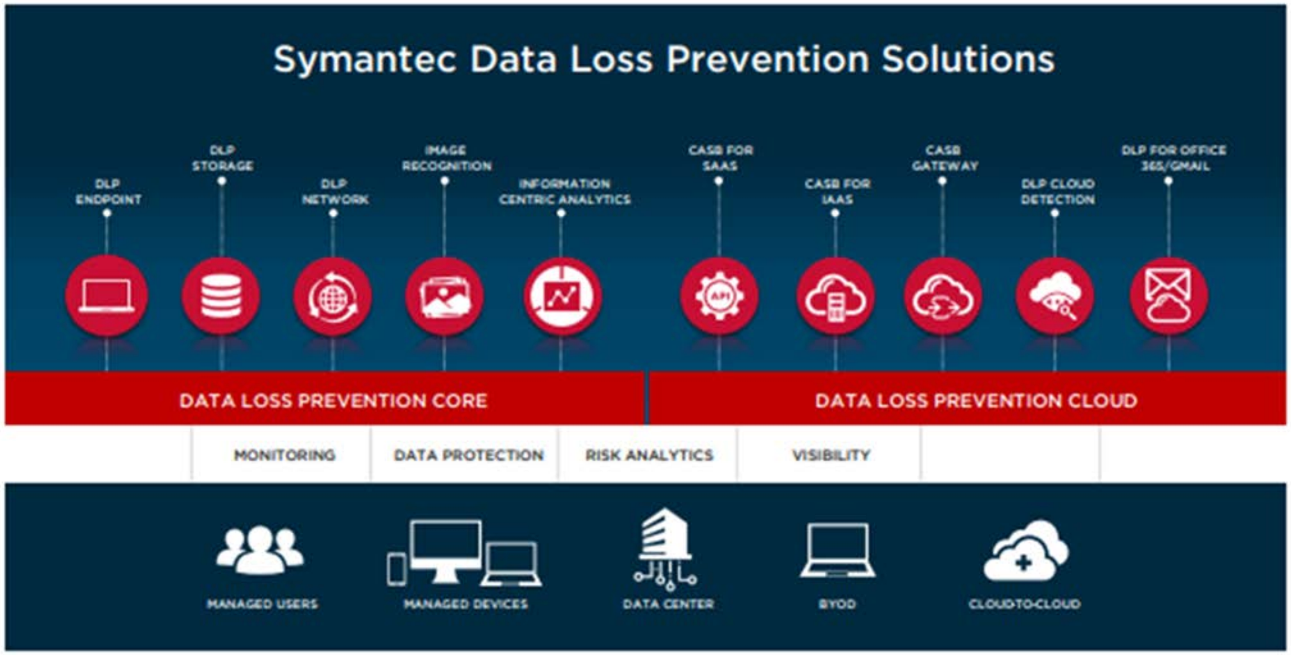
EXHIBIT K

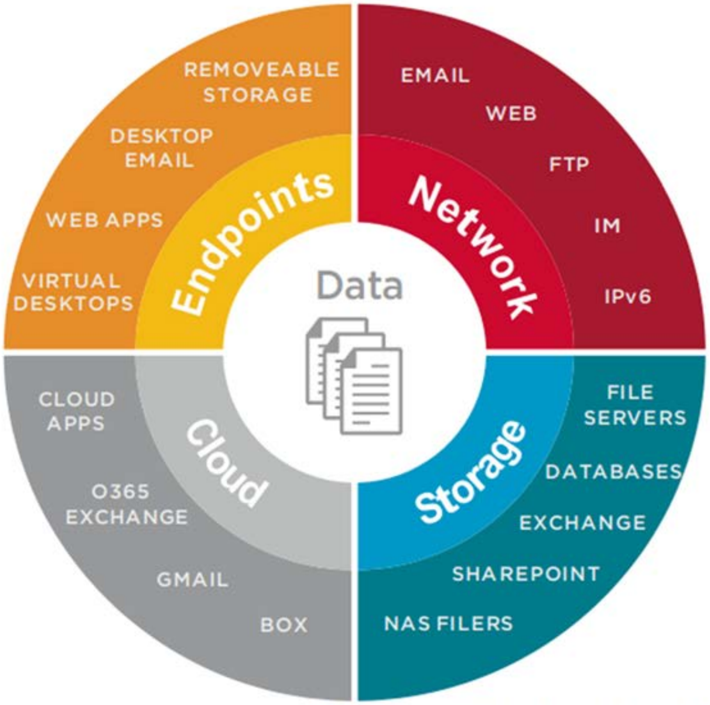
’840 Patent Infringement Claim Chart

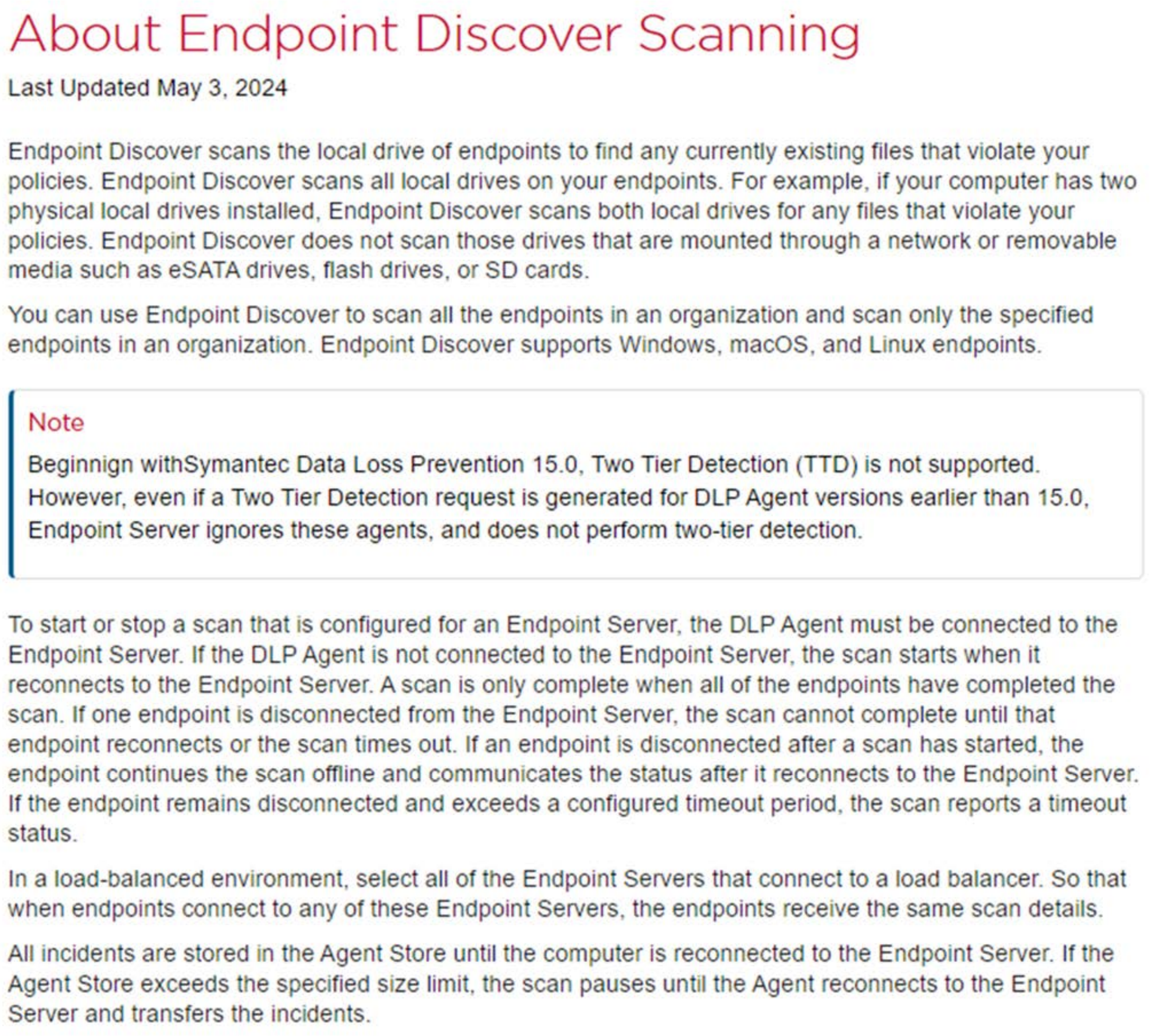
EXHIBIT K: U.S. PATENT NO. 11,637,840 INFRINGEMENT CLAIM CHART[1]

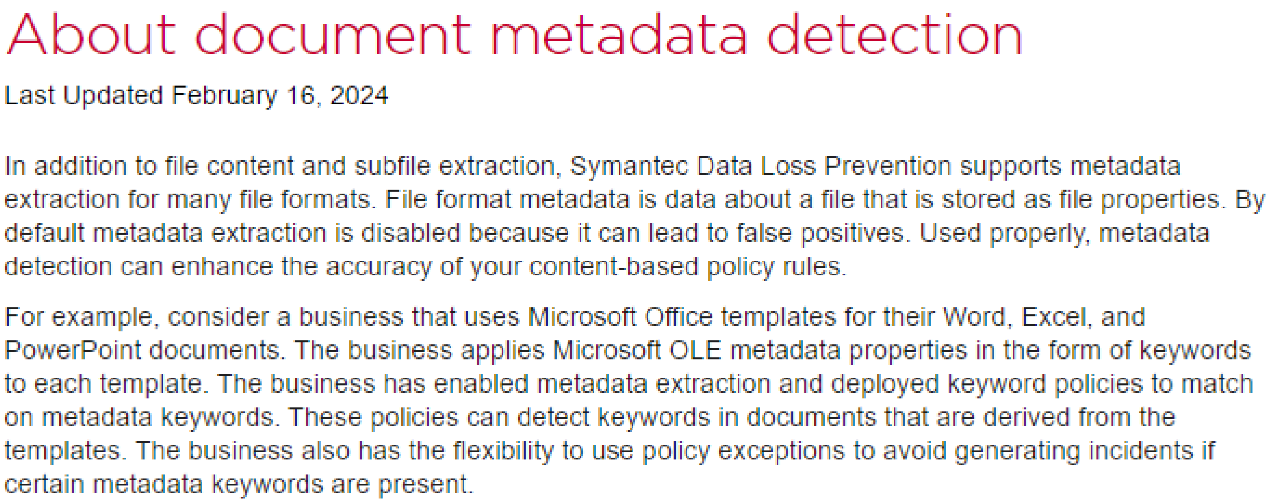
Claim 1	Symantec Enterprise Cloud
A computing system comprising	The preamble is presumptively not limiting. To the extent the preamble is limiting, Symantec Enterprise Cloud is a computing system.  Symantec Enterprise Cloud Buy via Partner Symantec Enterprise Cloud delivers data-centric hybrid security for the largest, most complex organizations in the world – on devices, in private data centers, and in the cloud. • **Consistent Compliance:** Apply and manage compliance controls consistently across the infrastructure. • **Secure Remote Work:** Protect critical enterprise assets wherever they live and from wherever they are accessed. • **Data and Threat Protection Everywhere:** Unify intelligence across control points to detect, block, and remediate targeted attacks. (https://www.broadcom.com/products/cybersecurity)

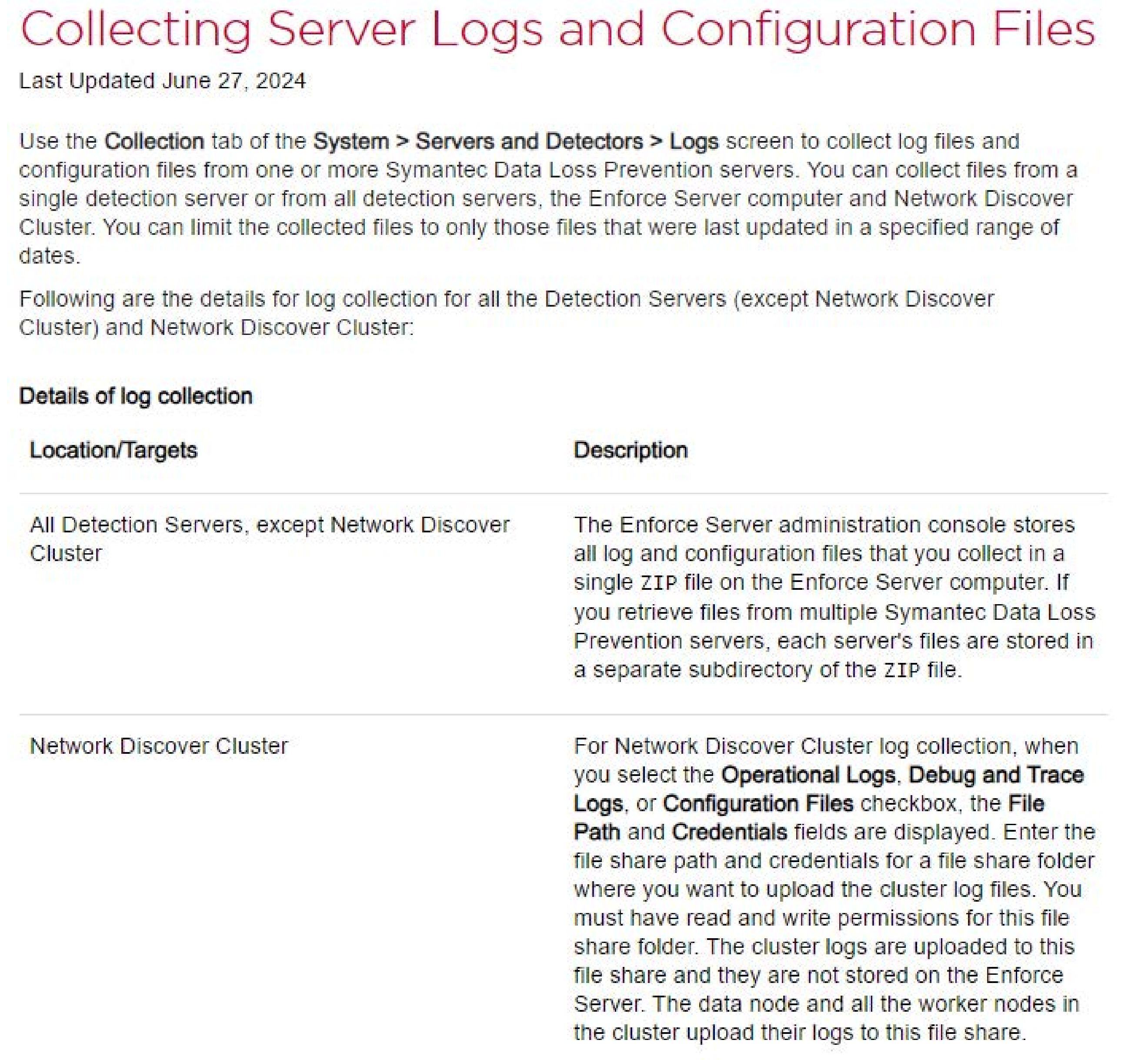
[1] The evidence of infringement identified in the below chart is exemplary and nonlimiting. QuickVault reserves the right to rely on additional and/or alternative aspects of Symantec Enterprise Cloud and related components during this litigation for the purpose of establishing infringement.

Claim 1	Symantec Enterprise Cloud
	 Symantec Data Loss Prevention Solutions DLP ENDPOINT DLP STORAGE DLP NETWORK IMAGE RECOGNITION INFORMATION CENTRIC ANALYTICS CASB FOR SAAS CASB FOR IAAS CASB GATEWAY DLP CLOUD DETECTION DLP FOR OFFICE 365/GMAIL API DATA LOSS PREVENTION CORE DATA LOSS PREVENTION CLOUD MONITORING DATA PROTECTION RISK ANALYTICS VISIBILITY MANAGED USERS MANAGED DEVICES DATA CENTER BYOD CLOUD-TO-CLOUD (https://docs.broadcom.com/doc/data-loss-prevention-family-en.)

Claim 1	Symantec Enterprise Cloud
one or more network devices, the one or more network devices comprising one or more microprocessors and one or more memories that store executable instructions that, when executed by the one or more microprocessors, facilitate performance of operations, comprising:	 REMOVEABLE STORAGE DESKTOP EMAIL WEB APPS VIRTUAL DESKTOPS Endpoints EMAIL WEB FTP IM IPv6 Network Data CLOUD APPS O365 EXCHANGE GMAIL BOX Cloud FILE SERVERS DATABASES EXCHANGE SHAREPOINT NAS FILERS Storage Symantec Data Loss Prevention (https://docs.broadcom.com/doc/data-loss-prevention-family-en.)

receiving meta data associated with an electronic file stored at an endpoint,	 About Endpoint Discover Scanning Last Updated May 3, 2024 Endpoint Discover scans the local drive of endpoints to find any currently existing files that violate your policies. Endpoint Discover scans all local drives on your endpoints. For example, if your computer has two physical local drives installed, Endpoint Discover scans both local drives for any files that violate your policies. Endpoint Discover does not scan those drives that are mounted through a network or removable media such as eSATA drives, flash drives, or SD cards. You can use Endpoint Discover to scan all the endpoints in an organization and scan only the specified endpoints in an organization. Endpoint Discover supports Windows, macOS, and Linux endpoints. Note Beginnign withSymantec Data Loss Prevention 15.0, Two Tier Detection (TTD) is not supported. However, even if a Two Tier Detection request is generated for DLP Agent versions earlier than 15.0, Endpoint Server ignores these agents, and does not perform two-tier detection. To start or stop a scan that is configured for an Endpoint Server, the DLP Agent must be connected to the Endpoint Server. If the DLP Agent is not connected to the Endpoint Server, the scan starts when it reconnects to the Endpoint Server. A scan is only complete when all of the endpoints have completed the scan. If one endpoint is disconnected from the Endpoint Server, the scan cannot complete until that endpoint reconnects or the scan times out. If an endpoint is disconnected after a scan has started, the endpoint continues the scan offline and communicates the status after it reconnects to the Endpoint Server. If the endpoint remains disconnected and exceeds a configured timeout period, the scan reports a timeout status. In a load-balanced environment, select all of the Endpoint Servers that connect to a load balancer. So that when endpoints connect to any of these Endpoint Servers, the endpoints receive the same scan details. All incidents are stored in the Agent Store until the computer is reconnected to the Endpoint Server. If the Agent Store exceeds the specified size limit, the scan pauses until the Agent reconnects to the Endpoint Server and transfers the incidents.

Claim 1	Symantec Enterprise Cloud
	(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-discovering-and-preventing-data-loss-on-endp-v98548126-d294e27/about-scanning-v16318536-d294e26629.html)
the metadata comprising: one or more of a file name associated with the electronic file, a creation date on which the electronic file was created, a modification date on which the electronic file was modified, one or more data element tags, and an endpoint identifier that is indicative of the endpoint on which the electronic file is located;	 About document metadata detection Last Updated February 16, 2024 In addition to file content and subfile extraction, Symantec Data Loss Prevention supports metadata extraction for many file formats. File format metadata is data about a file that is stored as file properties. By default metadata extraction is disabled because it can lead to false positives. Used properly, metadata detection can enhance the accuracy of your content-based policy rules. For example, consider a business that uses Microsoft Office templates for their Word, Excel, and PowerPoint documents. The business applies Microsoft OLE metadata properties in the form of keywords to each template. The business has enabled metadata extraction and deployed keyword policies to match on metadata keywords. These policies can detect keywords in documents that are derived from the templates. The business also has the flexibility to use policy exceptions to avoid generating incidents if certain metadata keywords are present. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-data-loss-prevention-policies-v27576413-d327e9/supported-file-formats-for-metadata-extraction-v77411276-d327e136440/about-document-metadata-detection-v77411550-d327e136433.html)



Collecting Server Logs and Configuration Files

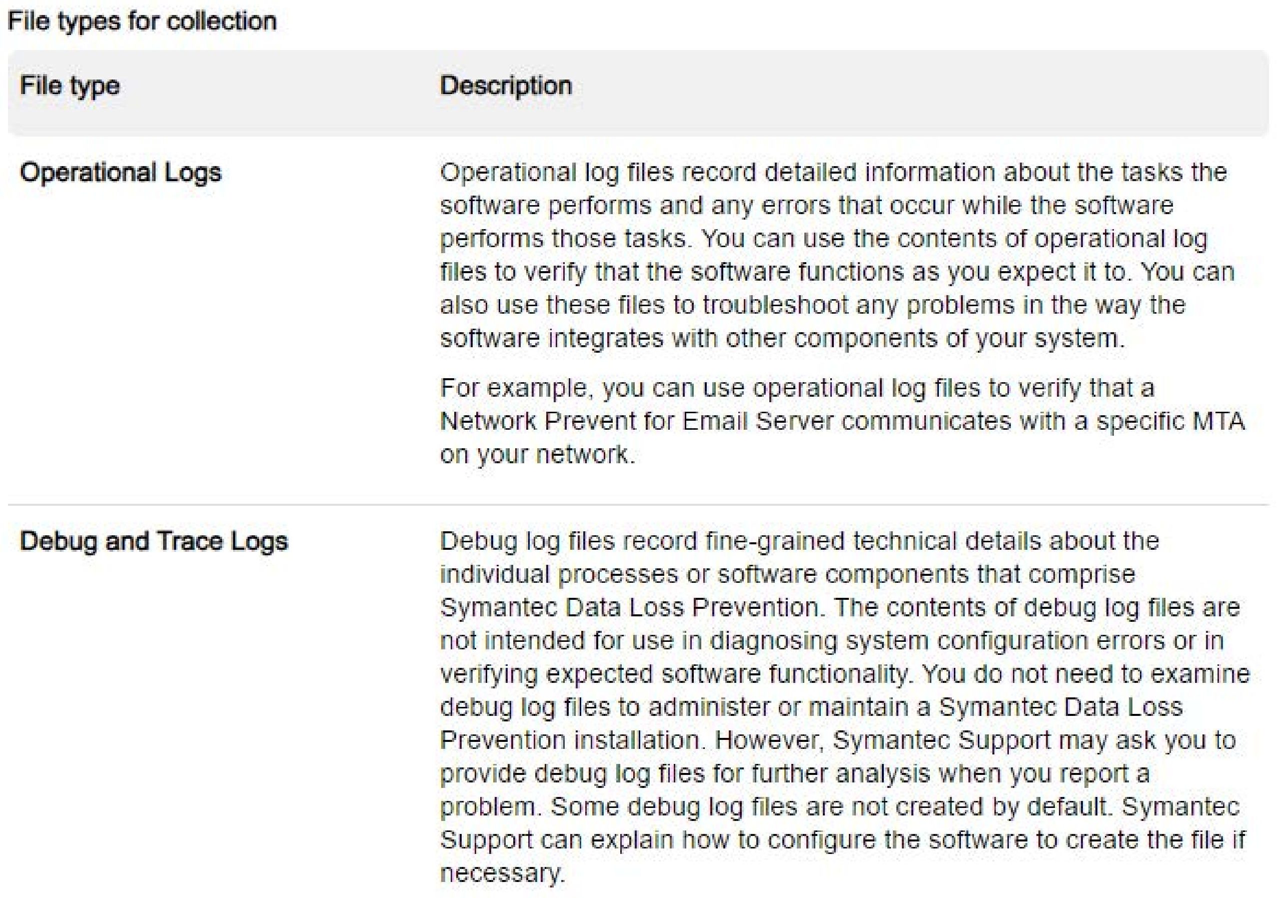
Last Updated June 27, 2024

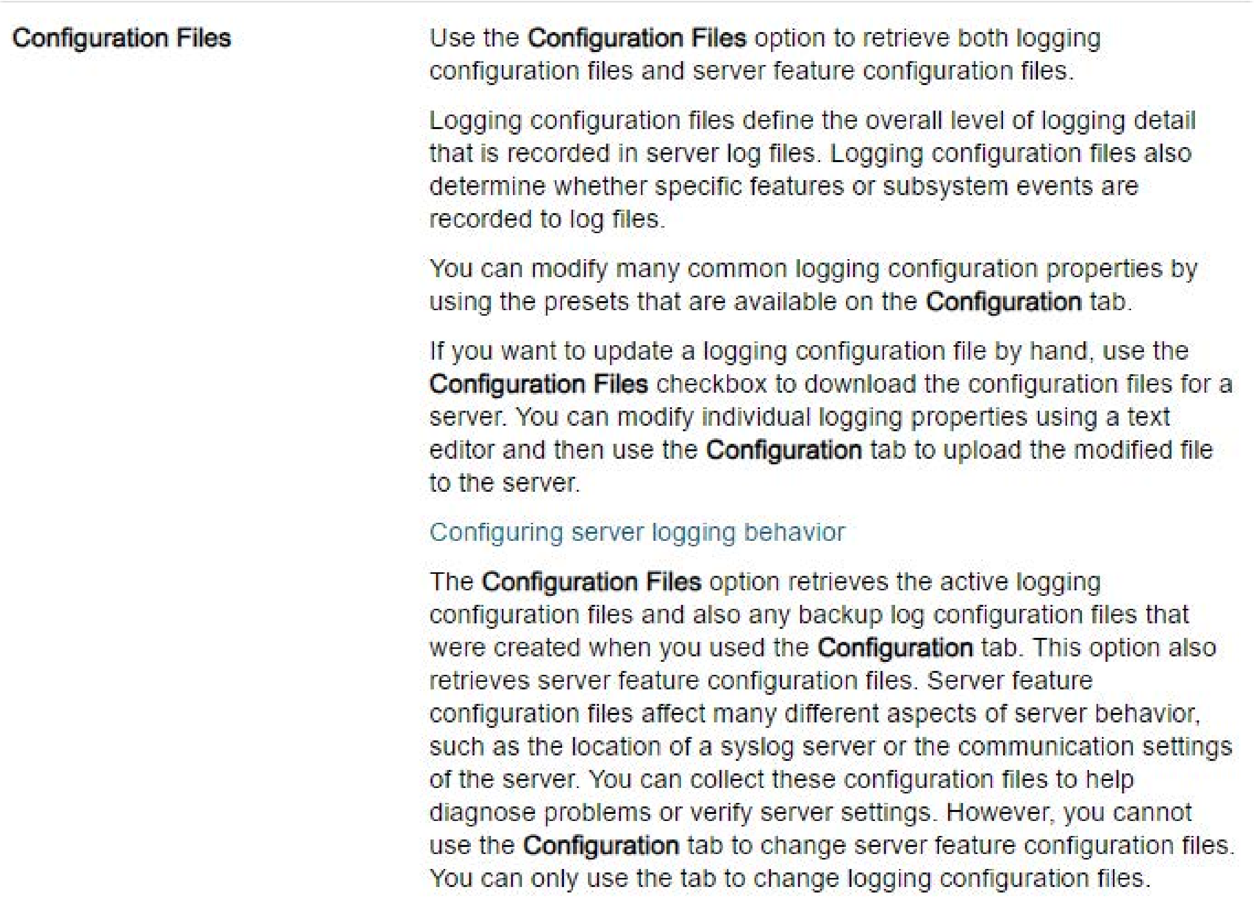
Use the **Collection** tab of the **System > Servers and Detectors > Logs** screen to collect log files and configuration files from one or more Symantec Data Loss Prevention servers. You can collect files from a single detection server or from all detection servers, the Enforce Server computer and Network Discover Cluster. You can limit the collected files to only those files that were last updated in a specified range of dates.

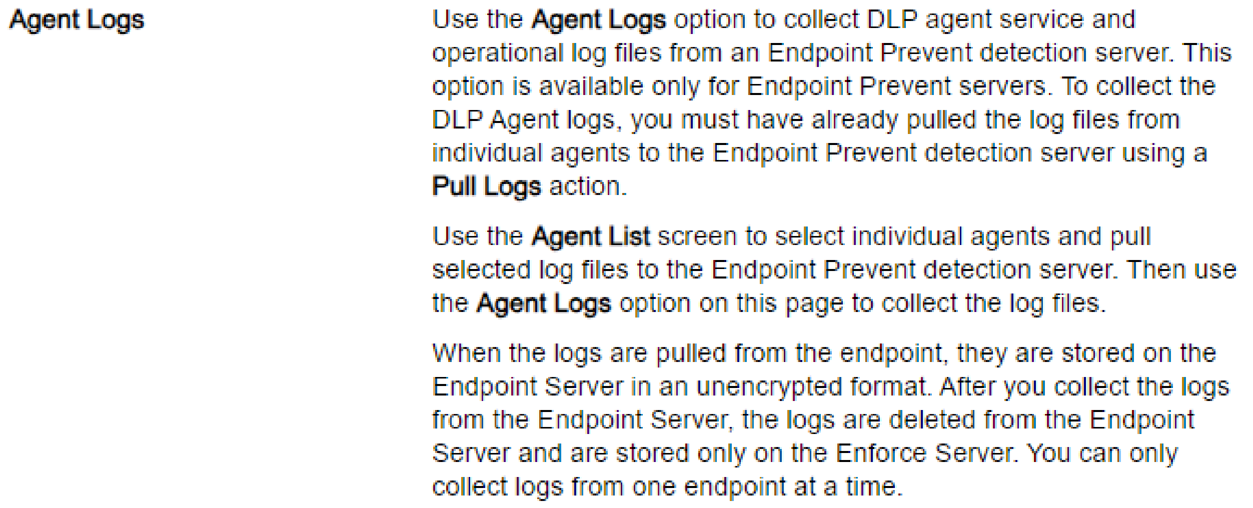
Following are the details for log collection for all the Detection Servers (except Network Discover Cluster) and Network Discover Cluster:

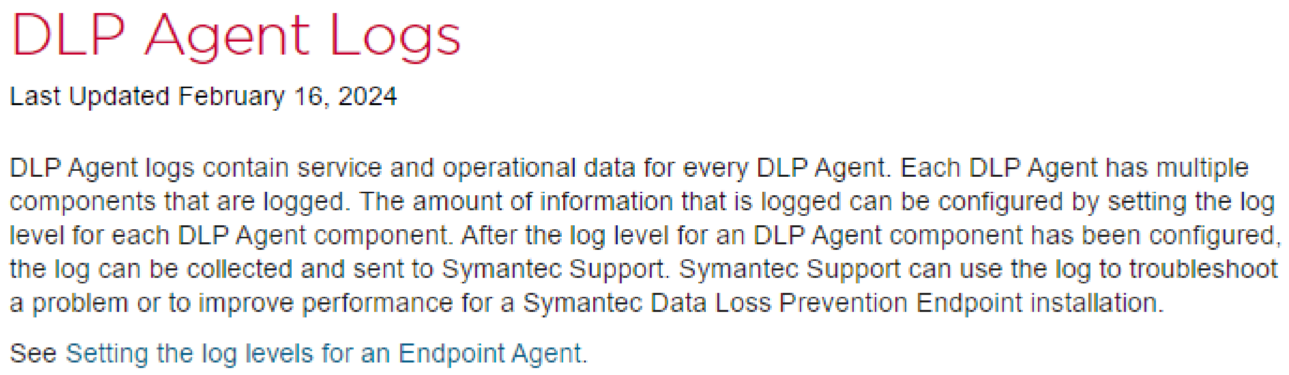
Details of log collection

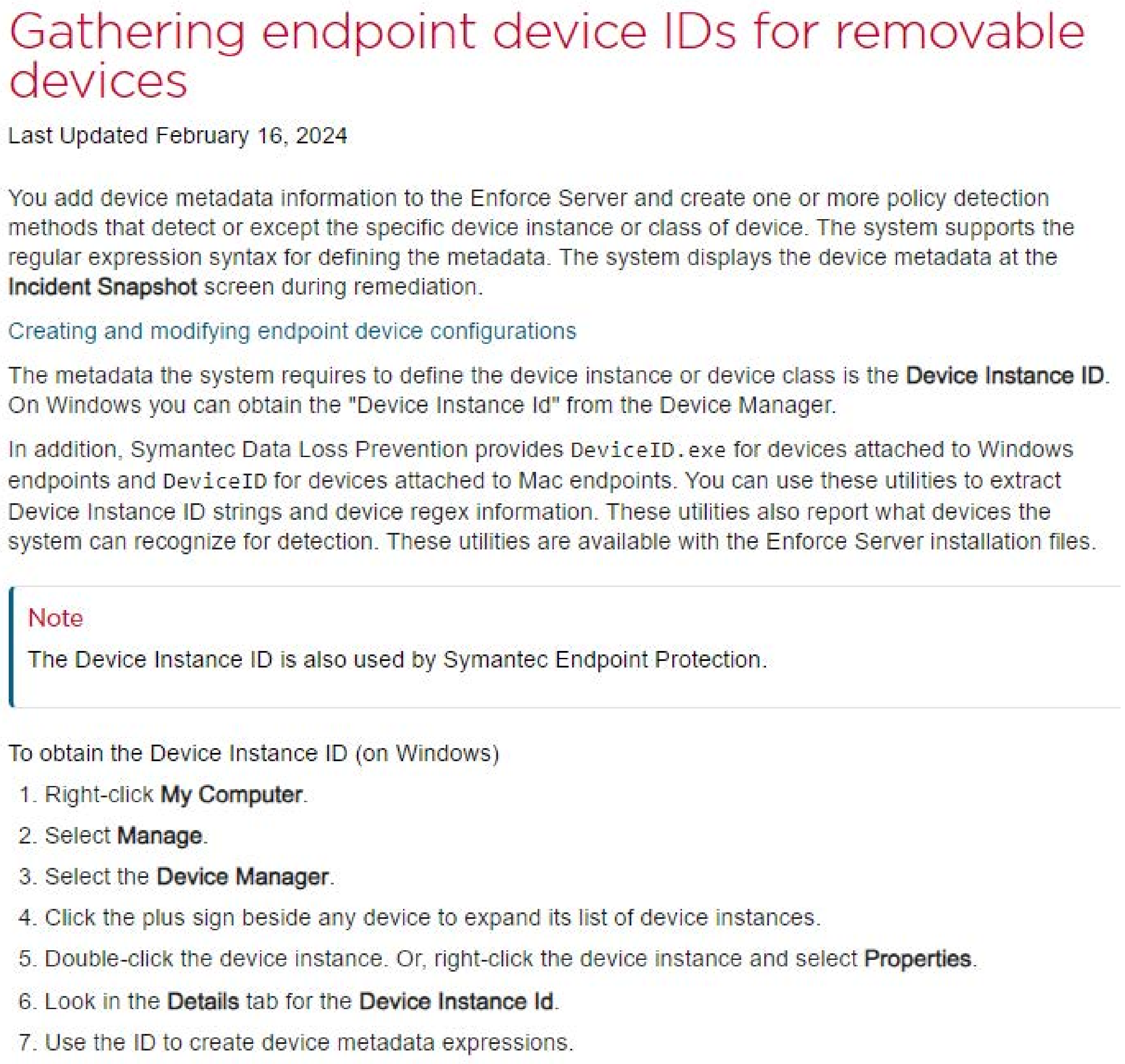
Location/Targets	Description
All Detection Servers, except Network Discover Cluster	The Enforce Server administration console stores all log and configuration files that you collect in a single `ZIP` file on the Enforce Server computer. If you retrieve files from multiple Symantec Data Loss Prevention servers, each server's files are stored in a separate subdirectory of the `ZIP` file.
Network Discover Cluster	For Network Discover Cluster log collection, when you select the **Operational Logs**, **Debug and Trace Logs**, or **Configuration Files** checkbox, the **File Path** and **Credentials** fields are displayed. Enter the file share path and credentials for a file share folder where you want to upload the cluster log files. You must have read and write permissions for this file share folder. The cluster logs are uploaded to this file share and they are not stored on the Enforce Server. The data node and all the worker nodes in the cluster upload their logs to this file share.

<table>
<tr><th>Claim 1</th><th>Symantec Enterprise Cloud</th></tr>
<tr><td></td><td>
File types for collection
<table>
<tr><th>File type</th><th>Description</th></tr>
<tr><td>Operational Logs</td><td>Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system.
For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network.</td></tr>
<tr><td>Debug and Trace Logs</td><td>Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain a Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary.</td></tr>
</table></td></tr>
</table>

Claim 1	Symantec Enterprise Cloud
	 **Configuration Files** Use the **Configuration Files** option to retrieve both logging configuration files and server feature configuration files. Logging configuration files define the overall level of logging detail that is recorded in server log files. Logging configuration files also determine whether specific features or subsystem events are recorded to log files. You can modify many common logging configuration properties by using the presets that are available on the **Configuration** tab. If you want to update a logging configuration file by hand, use the **Configuration Files** checkbox to download the configuration files for a server. You can modify individual logging properties using a text editor and then use the **Configuration** tab to upload the modified file to the server. Configuring server logging behavior The **Configuration Files** option retrieves the active logging configuration files and also any backup log configuration files that were created when you used the **Configuration** tab. This option also retrieves server feature configuration files. Server feature configuration files affect many different aspects of server behavior, such as the location of a syslog server or the communication settings of the server. You can collect these configuration files to help diagnose problems or verify server settings. However, you cannot use the **Configuration** tab to change server feature configuration files. You can only use the tab to change logging configuration files.

Claim 1	Symantec Enterprise Cloud
	 **Agent Logs** Use the **Agent Logs** option to collect DLP agent service and operational log files from an Endpoint Prevent detection server. This option is available only for Endpoint Prevent servers. To collect the DLP Agent logs, you must have already pulled the log files from individual agents to the Endpoint Prevent detection server using a **Pull Logs** action. Use the **Agent List** screen to select individual agents and pull selected log files to the Endpoint Prevent detection server. Then use the **Agent Logs** option on this page to collect the log files. When the logs are pulled from the endpoint, they are stored on the Endpoint Server in an unencrypted format. After you collect the logs from the Endpoint Server, the logs are deleted from the Endpoint Server and are stored only on the Enforce Server. You can only collect logs from one endpoint at a time. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/15-8/about-managing-servers-v15599809-d297e16684/collecting-server-logs-and-configuration-files-v33480324-d297e24269.html)

	 DLP Agent Logs Last Updated February 16, 2024 DLP Agent logs contain service and operational data for every DLP Agent. Each DLP Agent has multiple components that are logged. The amount of information that is logged can be configured by setting the log level for each DLP Agent component. After the log level for an DLP Agent component has been configured, the log can be collected and sent to Symantec Support. Symantec Support can use the log to troubleshoot a problem or to improve performance for a Symantec Data Loss Prevention Endpoint installation. See Setting the log levels for an Endpoint Agent. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/maintaining-the-system/understanding-underlying-system-resources-v15258948-d363e192/about-dlp-agent-logs-v75416710-d294e15012.html)



Gathering endpoint device IDs for removable devices

Last Updated February 16, 2024

You add device metadata information to the Enforce Server and create one or more policy detection methods that detect or except the specific device instance or class of device. The system supports the regular expression syntax for defining the metadata. The system displays the device metadata at the **Incident Snapshot** screen during remediation.

Creating and modifying endpoint device configurations

The metadata the system requires to define the device instance or device class is the **Device Instance ID**. On Windows you can obtain the "Device Instance Id" from the Device Manager.

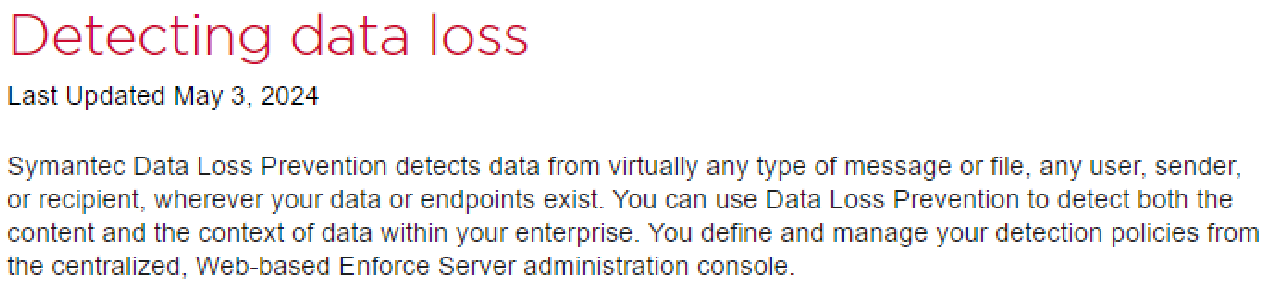
In addition, Symantec Data Loss Prevention provides `DeviceID.exe` for devices attached to Windows endpoints and `DeviceID` for devices attached to Mac endpoints. You can use these utilities to extract Device Instance ID strings and device regex information. These utilities also report what devices the system can recognize for detection. These utilities are available with the Enforce Server installation files.

> Note
>
> The Device Instance ID is also used by Symantec Endpoint Protection.

To obtain the Device Instance ID (on Windows)

1. Right-click **My Computer**.
2. Select **Manage**.
3. Select the **Device Manager**.
4. Click the plus sign beside any device to expand its list of device instances.
5. Double-click the device instance. Or, right-click the device instance and select **Properties**.
6. Look in the **Details** tab for the **Device Instance Id**.
7. Use the ID to create device metadata expressions.

(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-data-loss-prevention-policies-v27576413-d327e9/configuring-endpoint-event-detection-conditions-v85252962-d327e125553/gathering-endpoint-device-ids-for-removable-device-v42760780-d327e126068.html)

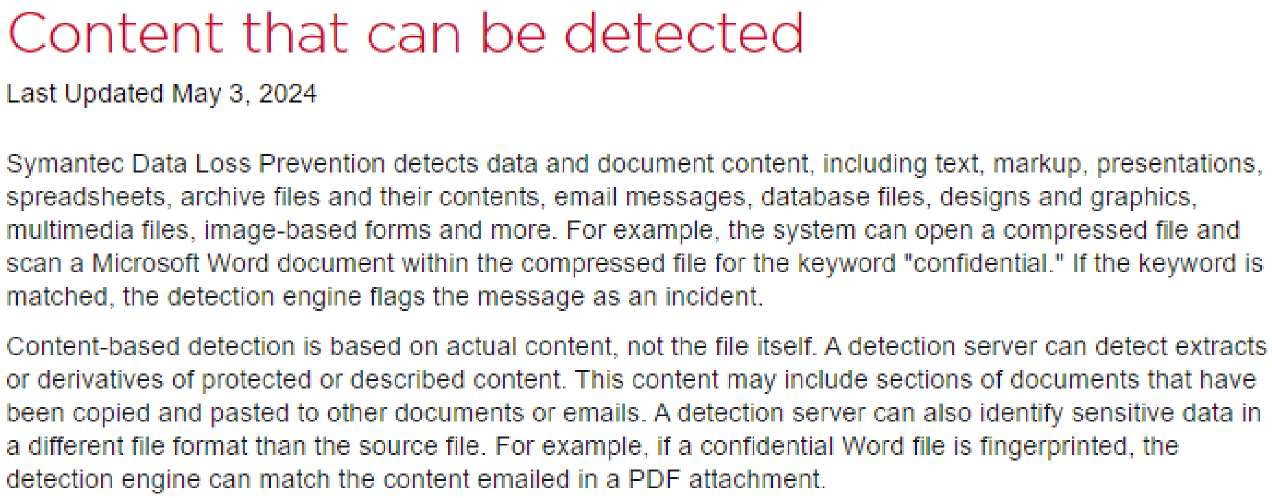


Detecting data loss

Last Updated May 3, 2024

Symantec Data Loss Prevention detects data from virtually any type of message or file, any user, sender, or recipient, wherever your data or endpoints exist. You can use Data Loss Prevention to detect both the content and the context of data within your enterprise. You define and manage your detection policies from the centralized, Web-based Enforce Server administration console.

(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/detecting-data-loss.html)



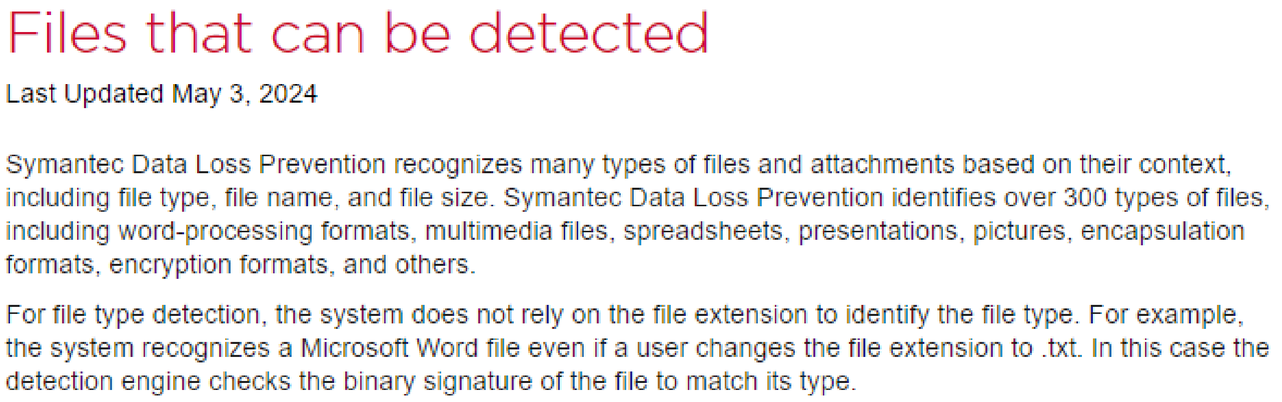
Content that can be detected

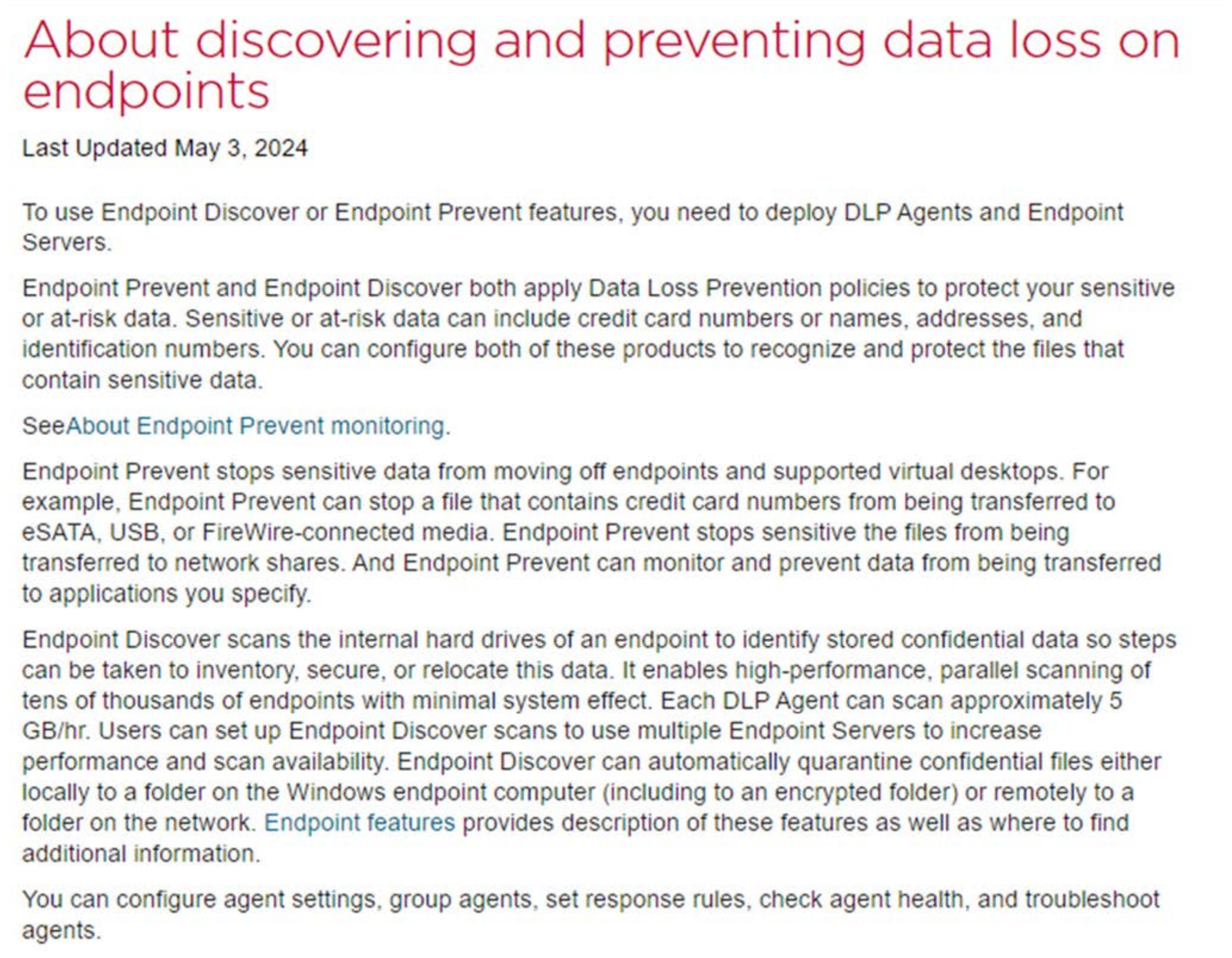
Last Updated May 3, 2024

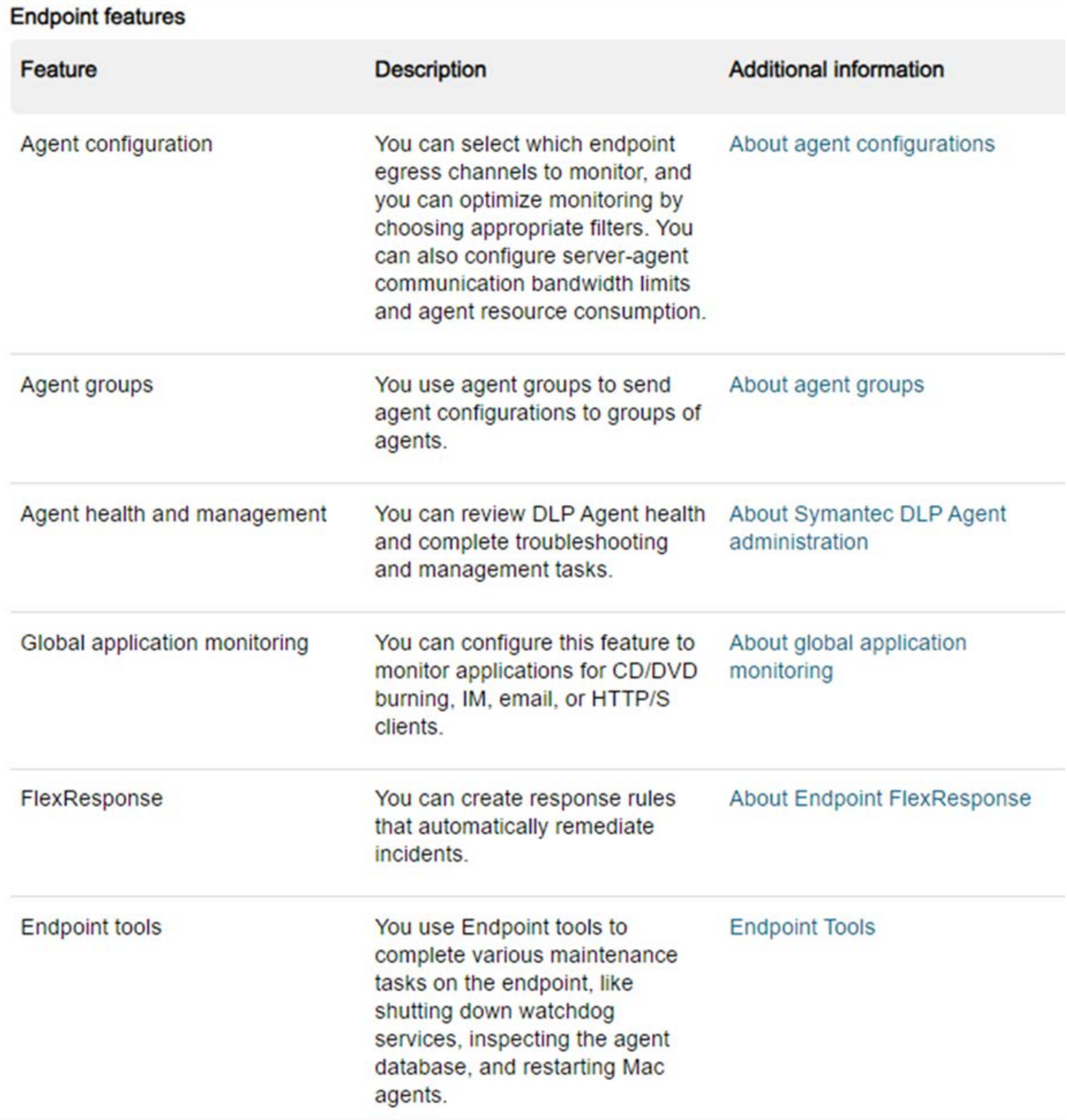
Symantec Data Loss Prevention detects data and document content, including text, markup, presentations, spreadsheets, archive files and their contents, email messages, database files, designs and graphics, multimedia files, image-based forms and more. For example, the system can open a compressed file and scan a Microsoft Word document within the compressed file for the keyword "confidential." If the keyword is matched, the detection engine flags the message as an incident.

Content-based detection is based on actual content, not the file itself. A detection server can detect extracts or derivatives of protected or described content. This content may include sections of documents that have been copied and pasted to other documents or emails. A detection server can also identify sensitive data in a different file format than the source file. For example, if a confidential Word file is fingerprinted, the detection engine can match the content emailed in a PDF attachment.

(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/detecting-data-loss/content-that-can-be-detected.html)

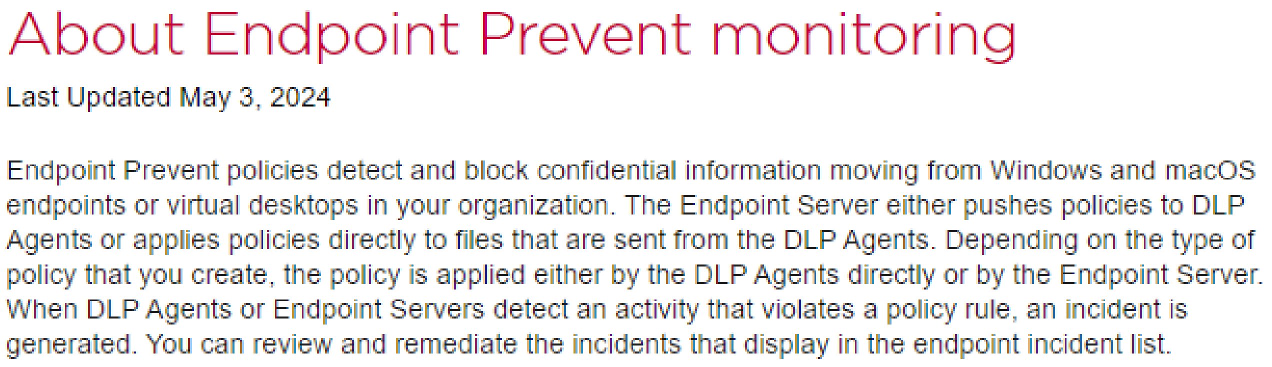
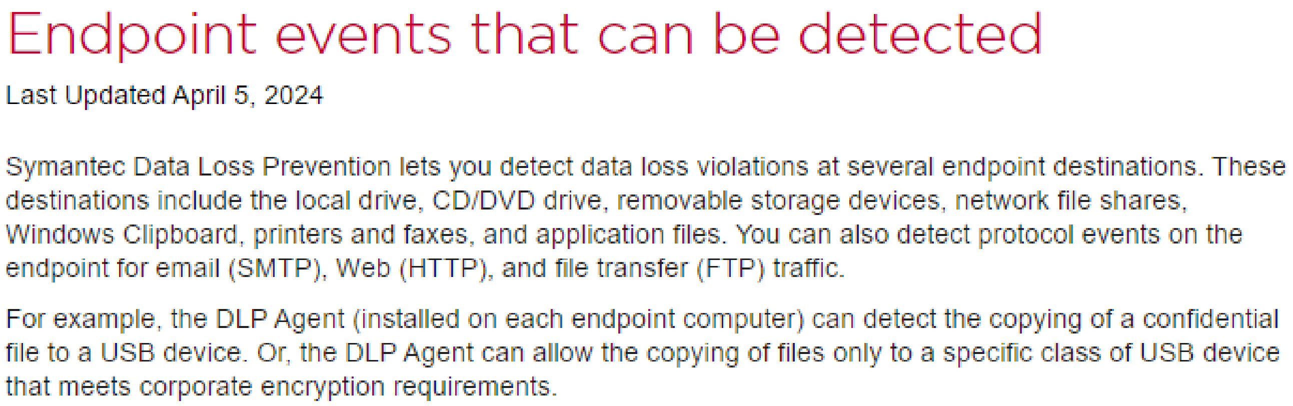
Claim 1	Symantec Enterprise Cloud
	 Files that can be detected Last Updated May 3, 2024 Symantec Data Loss Prevention recognizes many types of files and attachments based on their context, including file type, file name, and file size. Symantec Data Loss Prevention identifies over 300 types of files, including word-processing formats, multimedia files, spreadsheets, presentations, pictures, encapsulation formats, encryption formats, and others. For file type detection, the system does not rely on the file extension to identify the file type. For example, the system recognizes a Microsoft Word file even if a user changes the file extension to .txt. In this case the detection engine checks the binary signature of the file to match its type. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring/detecting-data-loss/files-that-can-be-detected.html)

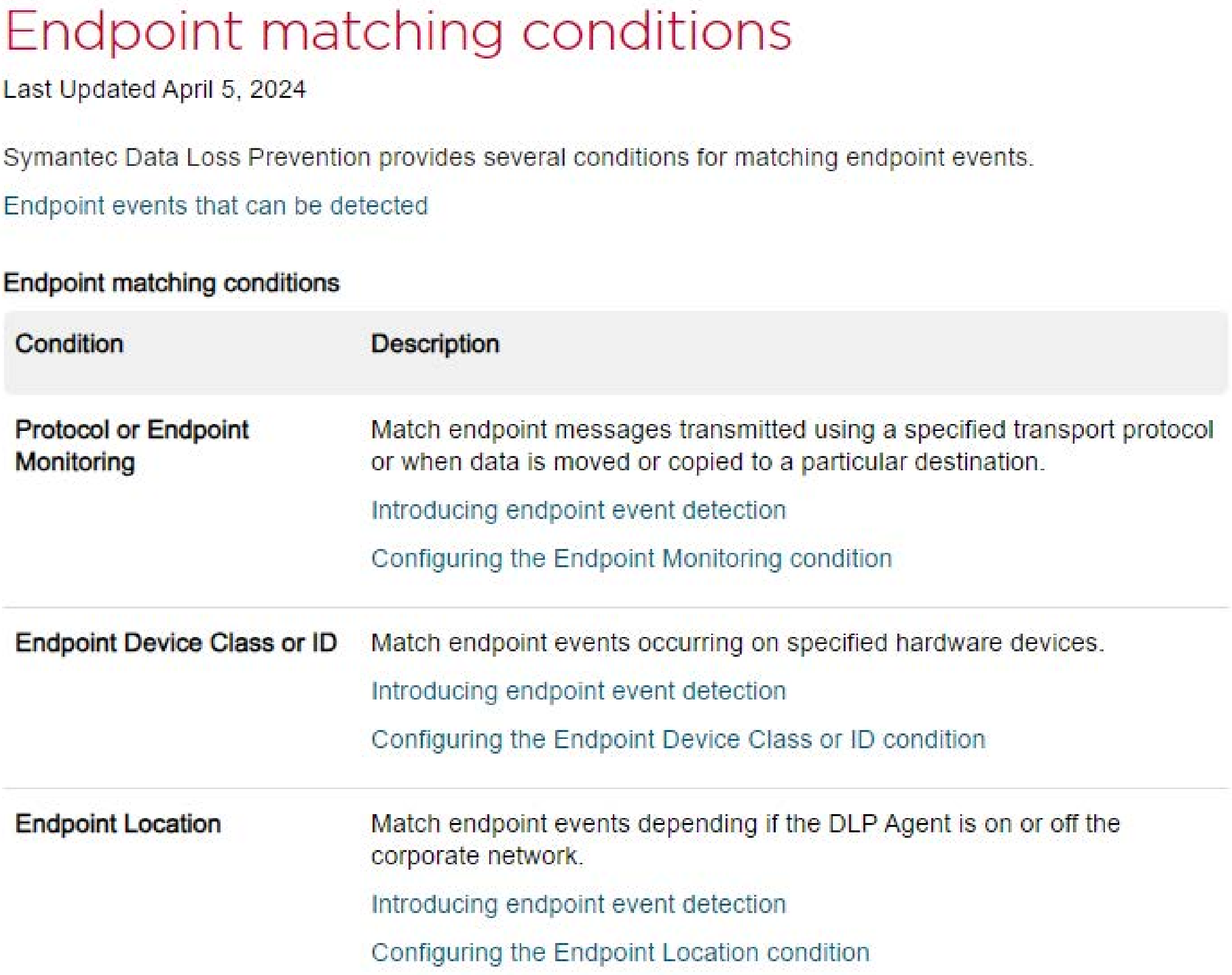
analyzing the meta data based on one or more of a configured setting and a policy;	 About discovering and preventing data loss on endpoints Last Updated May 3, 2024 To use Endpoint Discover or Endpoint Prevent features, you need to deploy DLP Agents and Endpoint Servers. Endpoint Prevent and Endpoint Discover both apply Data Loss Prevention policies to protect your sensitive or at-risk data. Sensitive or at-risk data can include credit card numbers or names, addresses, and identification numbers. You can configure both of these products to recognize and protect the files that contain sensitive data. SeeAbout Endpoint Prevent monitoring. Endpoint Prevent stops sensitive data from moving off endpoints and supported virtual desktops. For example, Endpoint Prevent can stop a file that contains credit card numbers from being transferred to eSATA, USB, or FireWire-connected media. Endpoint Prevent stops sensitive the files from being transferred to network shares. And Endpoint Prevent can monitor and prevent data from being transferred to applications you specify. Endpoint Discover scans the internal hard drives of an endpoint to identify stored confidential data so steps can be taken to inventory, secure, or relocate this data. It enables high-performance, parallel scanning of tens of thousands of endpoints with minimal system effect. Each DLP Agent can scan approximately 5 GB/hr. Users can set up Endpoint Discover scans to use multiple Endpoint Servers to increase performance and scan availability. Endpoint Discover can automatically quarantine confidential files either locally to a folder on the Windows endpoint computer (including to an encrypted folder) or remotely to a folder on the network. Endpoint features provides description of these features as well as where to find additional information. You can configure agent settings, group agents, set response rules, check agent health, and troubleshoot agents.



Endpoint features

Feature	Description	Additional information
Agent configuration	You can select which endpoint egress channels to monitor, and you can optimize monitoring by choosing appropriate filters. You can also configure server-agent communication bandwidth limits and agent resource consumption.	About agent configurations
Agent groups	You use agent groups to send agent configurations to groups of agents.	About agent groups
Agent health and management	You can review DLP Agent health and complete troubleshooting and management tasks.	About Symantec DLP Agent administration
Global application monitoring	You can configure this feature to monitor applications for CD/DVD burning, IM, email, or HTTP/S clients.	About global application monitoring
FlexResponse	You can create response rules that automatically remediate incidents.	About Endpoint FlexResponse
Endpoint tools	You use Endpoint tools to complete various maintenance tasks on the endpoint, like shutting down watchdog services, inspecting the agent database, and restarting Mac agents.	Endpoint Tools

Claim 1	Symantec Enterprise Cloud
	(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints.html)  About Endpoint Prevent monitoring Last Updated May 3, 2024 Endpoint Prevent policies detect and block confidential information moving from Windows and macOS endpoints or virtual desktops in your organization. The Endpoint Server either pushes policies to DLP Agents or applies policies directly to files that are sent from the DLP Agents. Depending on the type of policy that you create, the policy is applied either by the DLP Agents directly or by the Endpoint Server. When DLP Agents or Endpoint Servers detect an activity that violates a policy rule, an incident is generated. You can review and remediate the incidents that display in the endpoint incident list. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-prevent-monitoring.html)  Endpoint events that can be detected Last Updated April 5, 2024 Symantec Data Loss Prevention lets you detect data loss violations at several endpoint destinations. These destinations include the local drive, CD/DVD drive, removable storage devices, network file shares, Windows Clipboard, printers and faxes, and application files. You can also detect protocol events on the endpoint for email (SMTP), Web (HTTP), and file transfer (FTP) traffic. For example, the DLP Agent (installed on each endpoint computer) can detect the copying of a confidential file to a USB device. Or, the DLP Agent can allow the copying of files only to a specific class of USB device that meets corporate encryption requirements. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0/about-data-loss-prevention-policies-v27576413-d327e9/detecting-data-loss-v15598681-d327e1049/endpoint-events-that-can-be-detected-v40065947-d327e1125.html)

<table>
<tr><th>Claim 1</th><th>Symantec Enterprise Cloud</th></tr>
<tr><td></td><td>


Endpoint matching conditions

Last Updated April 5, 2024

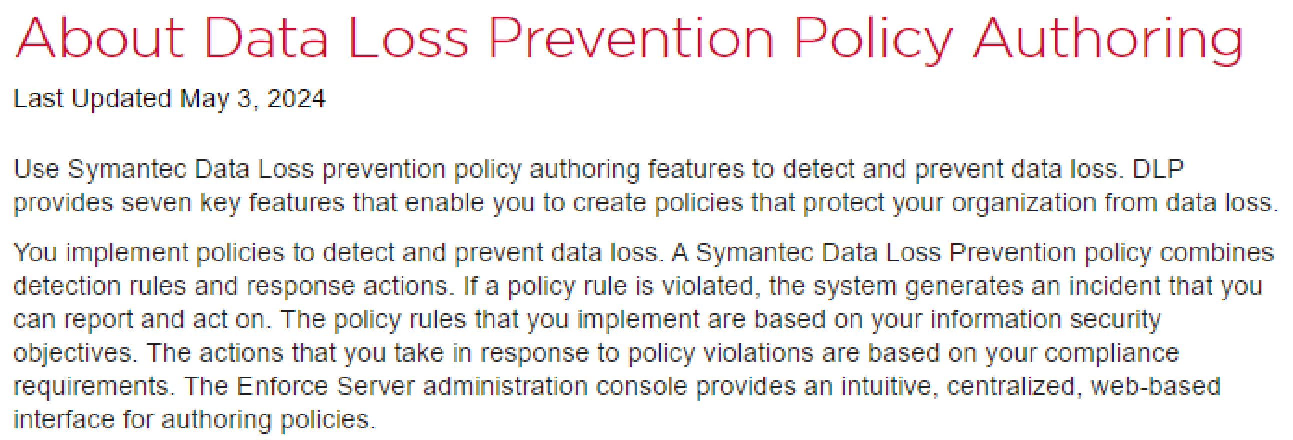
Symantec Data Loss Prevention provides several conditions for matching endpoint events.

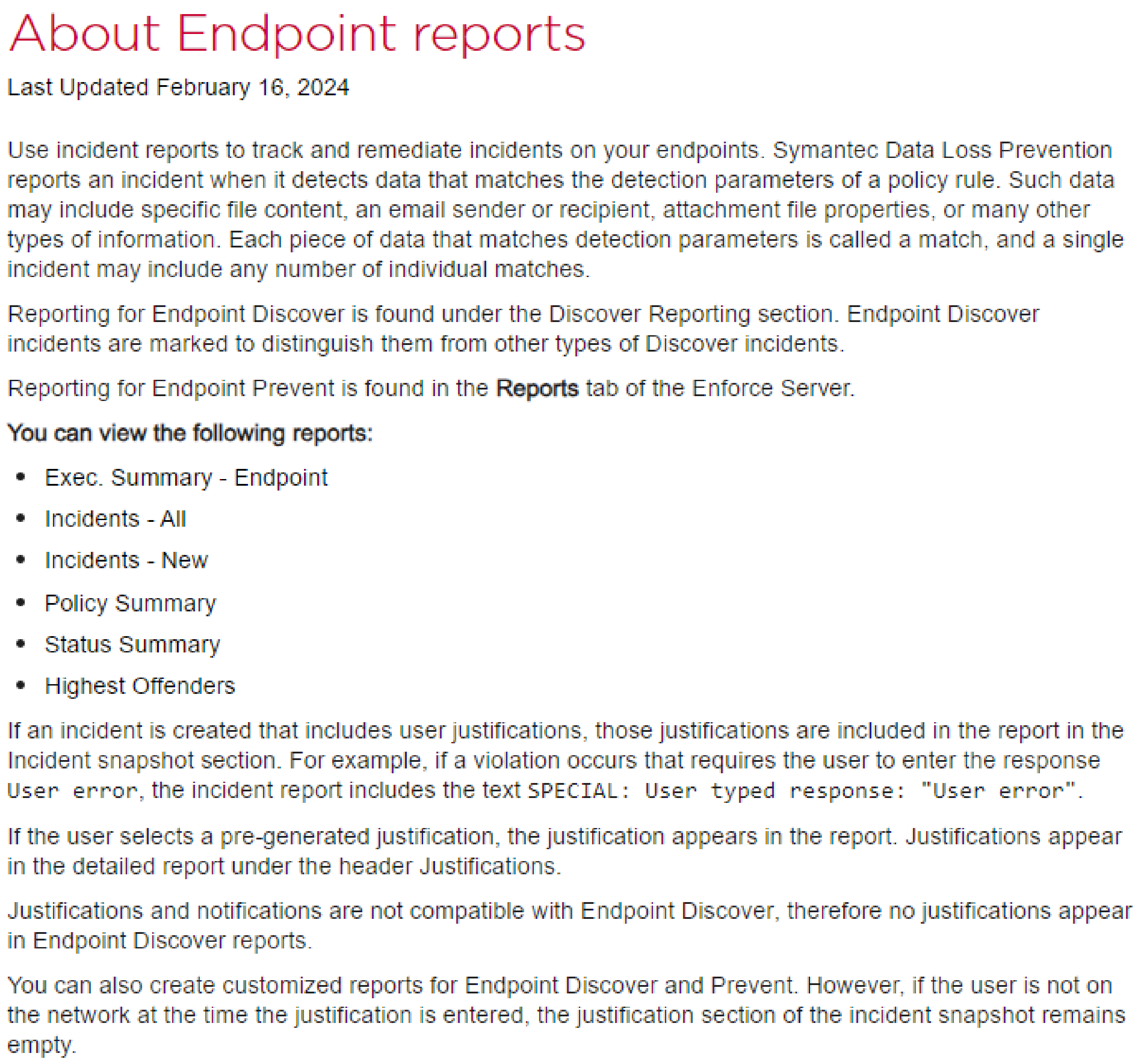
Endpoint events that can be detected

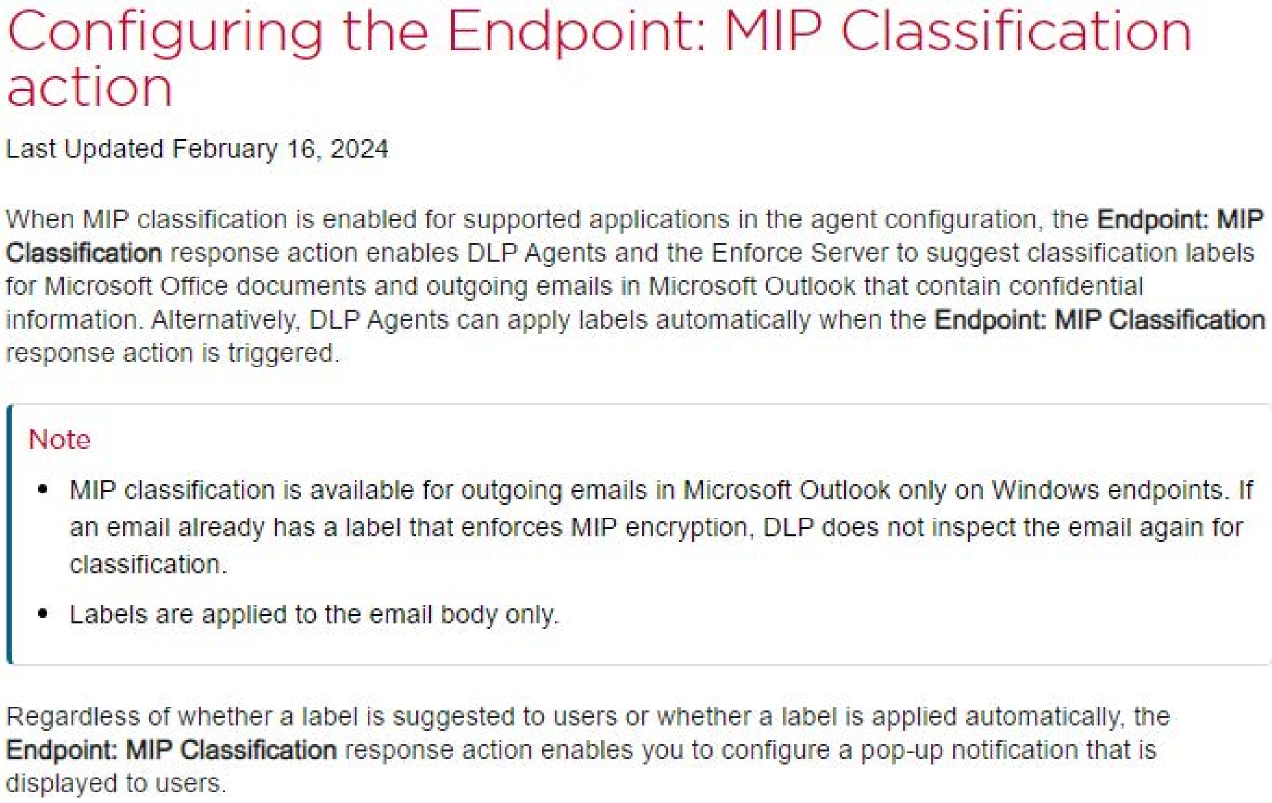
Endpoint matching conditions

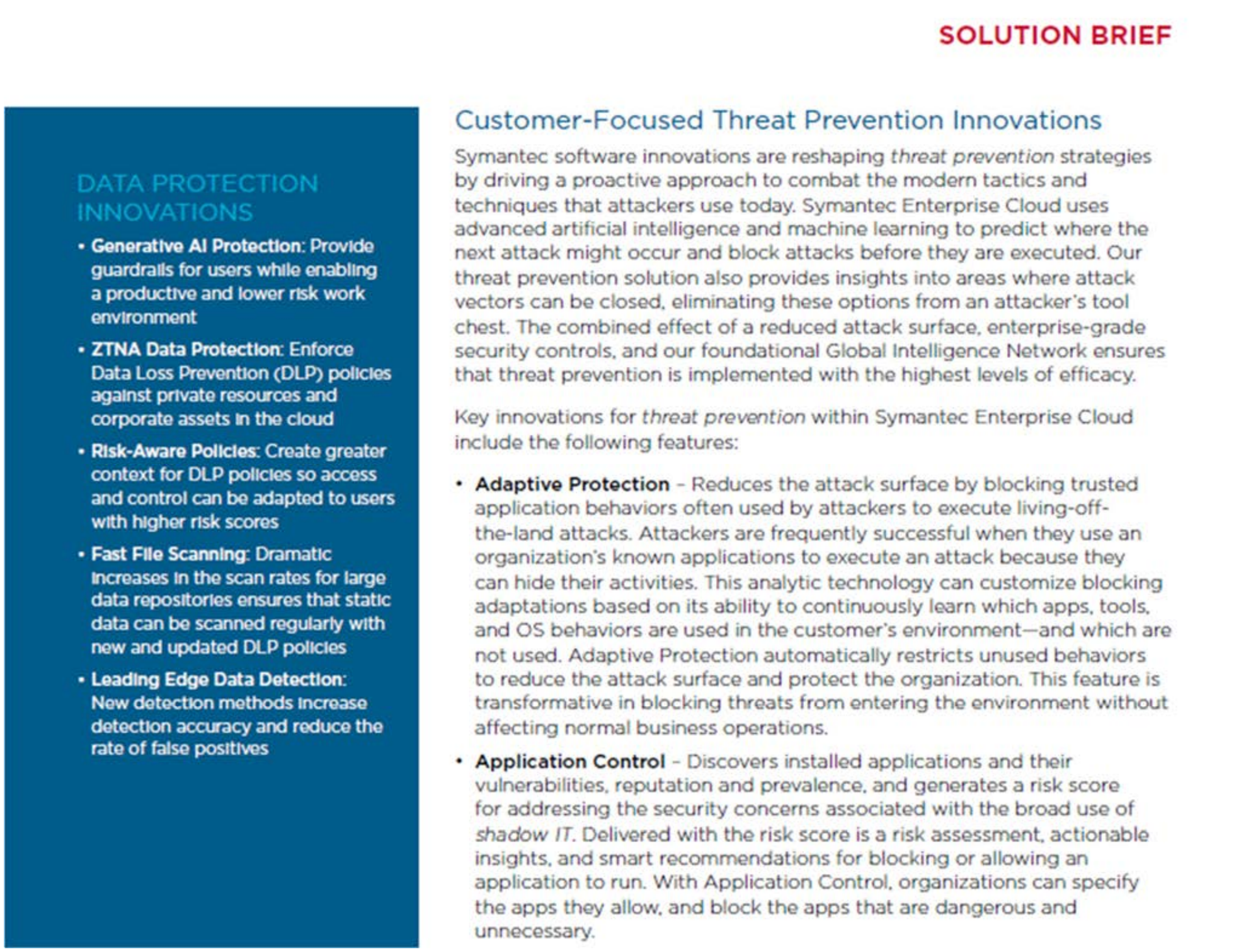
<table>
<tr><th>Condition</th><th>Description</th></tr>
<tr><td><b>Protocol or Endpoint Monitoring</b></td><td>Match endpoint messages transmitted using a specified transport protocol or when data is moved or copied to a particular destination.
Introducing endpoint event detection
Configuring the Endpoint Monitoring condition</td></tr>
<tr><td><b>Endpoint Device Class or ID</b></td><td>Match endpoint events occurring on specified hardware devices.
Introducing endpoint event detection
Configuring the Endpoint Device Class or ID condition</td></tr>
<tr><td><b>Endpoint Location</b></td><td>Match endpoint events depending if the DLP Agent is on or off the corporate network.
Introducing endpoint event detection
Configuring the Endpoint Location condition</td></tr>
</table>

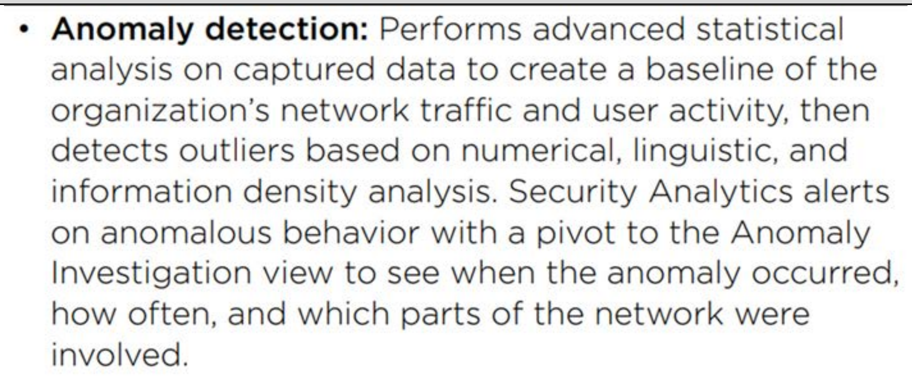
(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0/about-data-loss-prevention-policies-v27576413-d327e9/policy-matching-conditions-v40499624-d327e1698/endpoint-matching-conditions-v41286484-d327e2045.html#v41286484)
</td></tr>
</table>

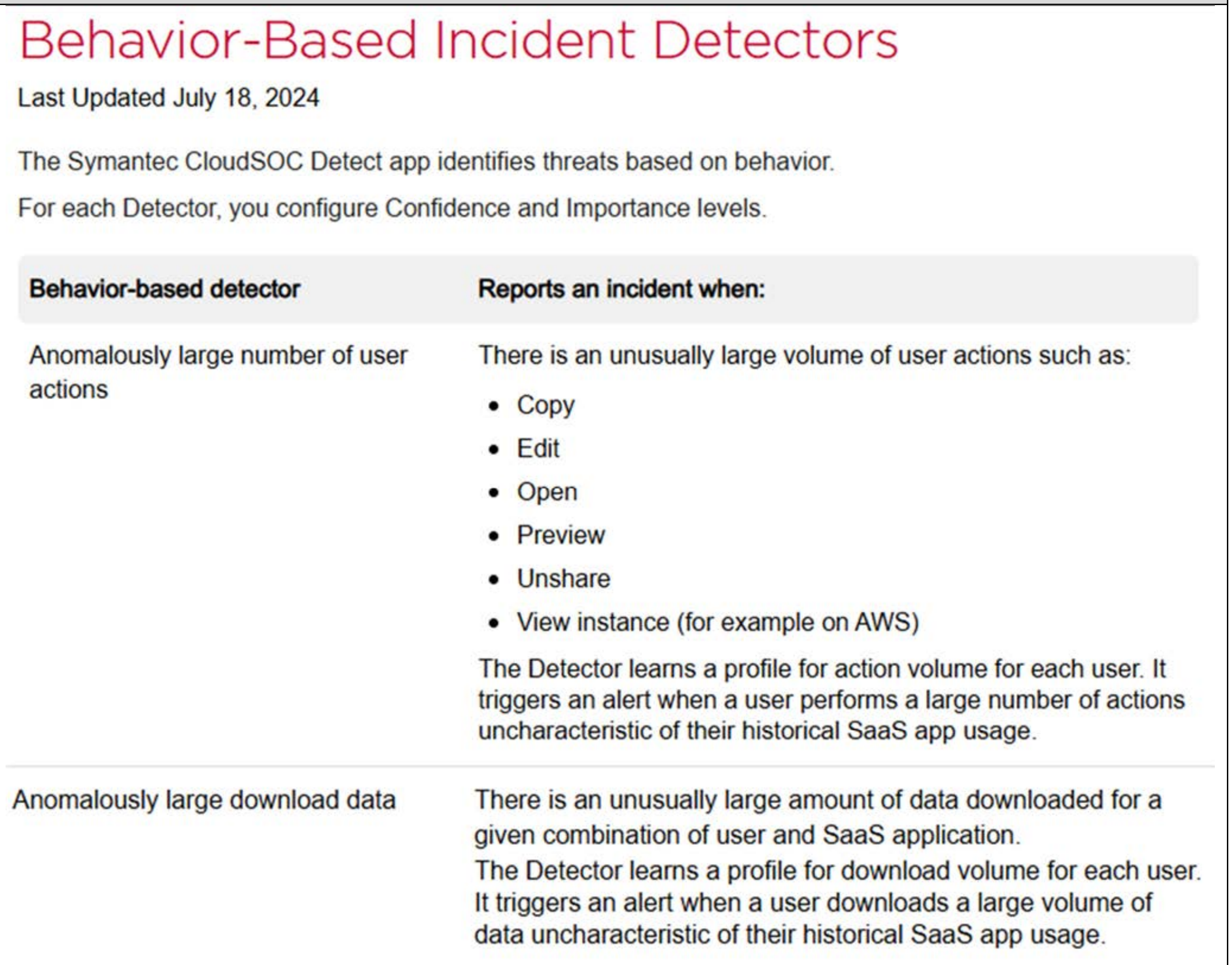
Claim 1	Symantec Enterprise Cloud
	 About Data Loss Prevention Policy Authoring Last Updated May 3, 2024 Use Symantec Data Loss prevention policy authoring features to detect and prevent data loss. DLP provides seven key features that enable you to create policies that protect your organization from data loss. You implement policies to detect and prevent data loss. A Symantec Data Loss Prevention policy combines detection rules and response actions. If a policy rule is violated, the system generates an incident that you can report and act on. The policy rules that you implement are based on your information security objectives. The actions that you take in response to policy violations are based on your compliance requirements. The Enforce Server administration console provides an intuitive, centralized, web-based interface for authoring policies. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-data-loss-prevention-policy-authoring.html)

determining, based on the analyzing of the meta data, a data classification associated with the electronic file;	 About Endpoint reports Last Updated February 16, 2024 Use incident reports to track and remediate incidents on your endpoints. Symantec Data Loss Prevention reports an incident when it detects data that matches the detection parameters of a policy rule. Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information. Each piece of data that matches detection parameters is called a match, and a single incident may include any number of individual matches. Reporting for Endpoint Discover is found under the Discover Reporting section. Endpoint Discover incidents are marked to distinguish them from other types of Discover incidents. Reporting for Endpoint Prevent is found in the **Reports** tab of the Enforce Server. **You can view the following reports:** • Exec. Summary - Endpoint • Incidents - All • Incidents - New • Policy Summary • Status Summary • Highest Offenders If an incident is created that includes user justifications, those justifications are included in the report in the Incident snapshot section. For example, if a violation occurs that requires the user to enter the response `User error`, the incident report includes the text `SPECIAL: User typed response: "User error"`. If the user selects a pre-generated justification, the justification appears in the report. Justifications appear in the detailed report under the header Justifications. Justifications and notifications are not compatible with Endpoint Discover, therefore no justifications appear in Endpoint Discover reports. You can also create customized reports for Endpoint Discover and Prevent. However, if the user is not on the network at the time the justification is entered, the justification section of the incident snapshot remains empty.

Claim 1	Symantec Enterprise Cloud
	(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-discovering-and-preventing-data-loss-on-endp-v98548126-d294e27/managing-target-scans-v97535512-d294e27271/about-endpoint-reports-v15602064-d294e366.html)  Configuring the Endpoint: MIP Classification action Last Updated February 16, 2024 When MIP classification is enabled for supported applications in the agent configuration, the **Endpoint: MIP Classification** response action enables DLP Agents and the Enforce Server to suggest classification labels for Microsoft Office documents and outgoing emails in Microsoft Outlook that contain confidential information. Alternatively, DLP Agents can apply labels automatically when the **Endpoint: MIP Classification** response action is triggered. Note • MIP classification is available for outgoing emails in Microsoft Outlook only on Windows endpoints. If an email already has a label that enforces MIP encryption, DLP does not inspect the email again for classification. • Labels are applied to the email body only. Regardless of whether a label is suggested to users or whether a label is applied automatically, the **Endpoint: MIP Classification** response action enables you to configure a pop-up notification that is displayed to users. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1/about-response-rules-v40462357-d339e11/Configuring-the-Endpoint--MIP-Classification-action-.html)

Claim 1	Symantec Enterprise Cloud
further determining, based on the analyzing of the meta data, that the electronic file is unauthorized due to a pattern of data use that constitutes a deviation from normal behavior, wherein the deviation from normal behavior is a discovery that the endpoint has increased a total number of files by a percentage that exceeds an average for a user associated with the endpoint or for an average user;	 SOLUTION BRIEF DATA PROTECTION INNOVATIONS • **Generative AI Protection**: Provide guardrails for users while enabling a productive and lower risk work environment • **ZTNA Data Protection**: Enforce Data Loss Prevention (DLP) policies against private resources and corporate assets in the cloud • **Risk-Aware Policies**: Create greater context for DLP policies so access and control can be adapted to users with higher risk scores • **Fast File Scanning**: Dramatic increases in the scan rates for large data repositories ensures that static data can be scanned regularly with new and updated DLP policies • **Leading Edge Data Detection**: New detection methods increase detection accuracy and reduce the rate of false positives Customer-Focused Threat Prevention Innovations Symantec software innovations are reshaping *threat prevention* strategies by driving a proactive approach to combat the modern tactics and techniques that attackers use today. Symantec Enterprise Cloud uses advanced artificial intelligence and machine learning to predict where the next attack might occur and block attacks before they are executed. Our threat prevention solution also provides insights into areas where attack vectors can be closed, eliminating these options from an attacker's tool chest. The combined effect of a reduced attack surface, enterprise-grade security controls, and our foundational Global Intelligence Network ensures that threat prevention is implemented with the highest levels of efficacy. Key innovations for *threat prevention* within Symantec Enterprise Cloud include the following features: • **Adaptive Protection** – Reduces the attack surface by blocking trusted application behaviors often used by attackers to execute living-off-the-land attacks. Attackers are frequently successful when they use an organization's known applications to execute an attack because they can hide their activities. This analytic technology can customize blocking adaptations based on its ability to continuously learn which apps, tools, and OS behaviors are used in the customer's environment—and which are not used. Adaptive Protection automatically restricts unused behaviors to reduce the attack surface and protect the organization. This feature is transformative in blocking threats from entering the environment without affecting normal business operations. • **Application Control** – Discovers installed applications and their vulnerabilities, reputation and prevalence, and generates a risk score for addressing the security concerns associated with the broad use of *shadow IT*. Delivered with the risk score is a risk assessment, actionable insights, and smart recommendations for blocking or allowing an application to run. With Application Control, organizations can specify the apps they allow, and block the apps that are dangerous and unnecessary. (https://docs.broadcom.com/doc/threat-prevention-and-data-protection)

Claim 1	Symantec Enterprise Cloud
	 • **Anomaly detection:** Performs advanced statistical analysis on captured data to create a baseline of the organization's network traffic and user activity, then detects outliers based on numerical, linguistic, and information density analysis. Security Analytics alerts on anomalous behavior with a pivot to the Anomaly Investigation view to see when the anomaly occurred, how often, and which parts of the network were involved. (https://docs.broadcom.com/doc/security-analytics-appliances-en)

Claim 1	Symantec Enterprise Cloud
	

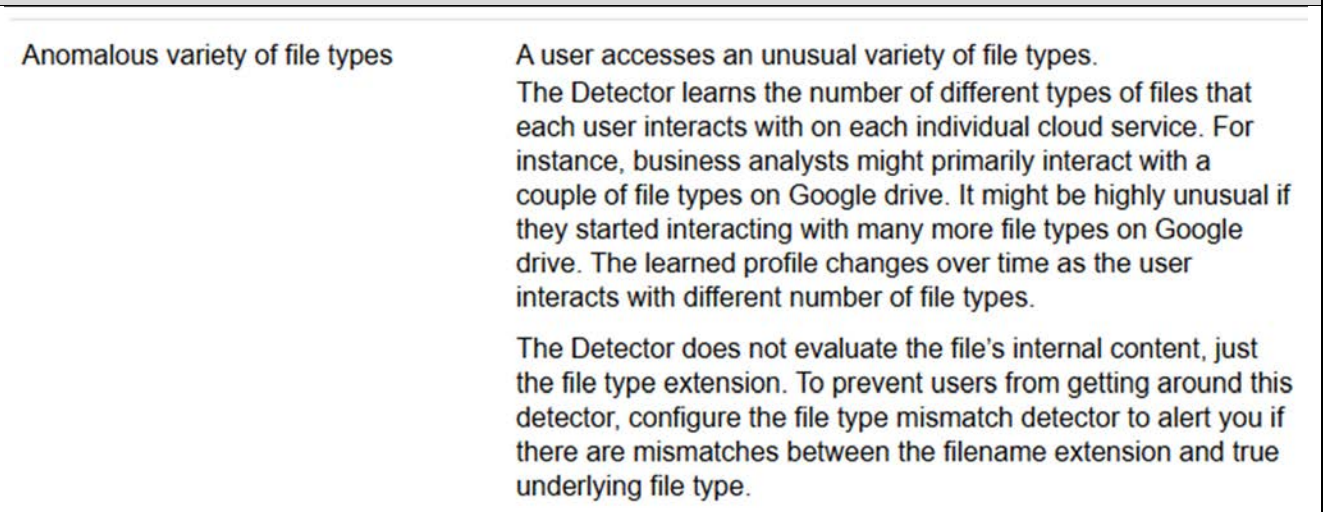
Behavior-Based Incident Detectors

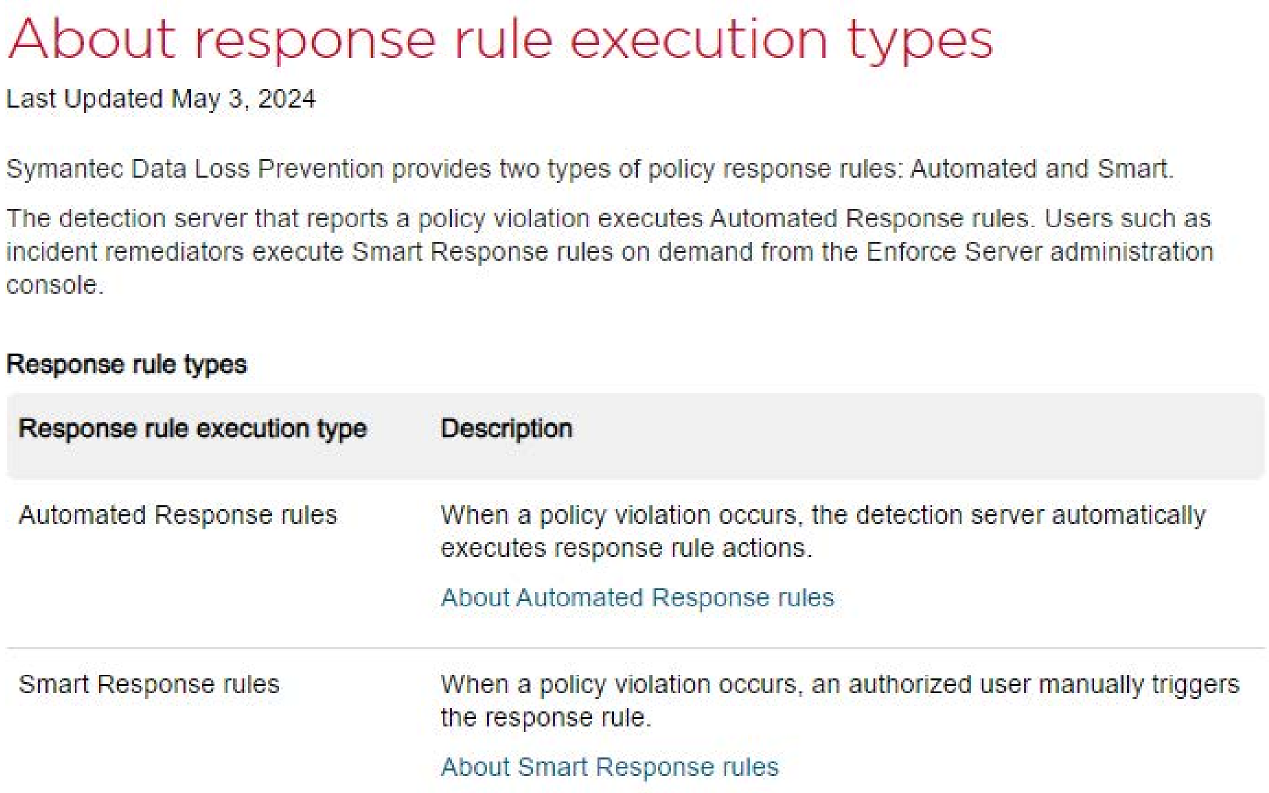
Last Updated July 18, 2024

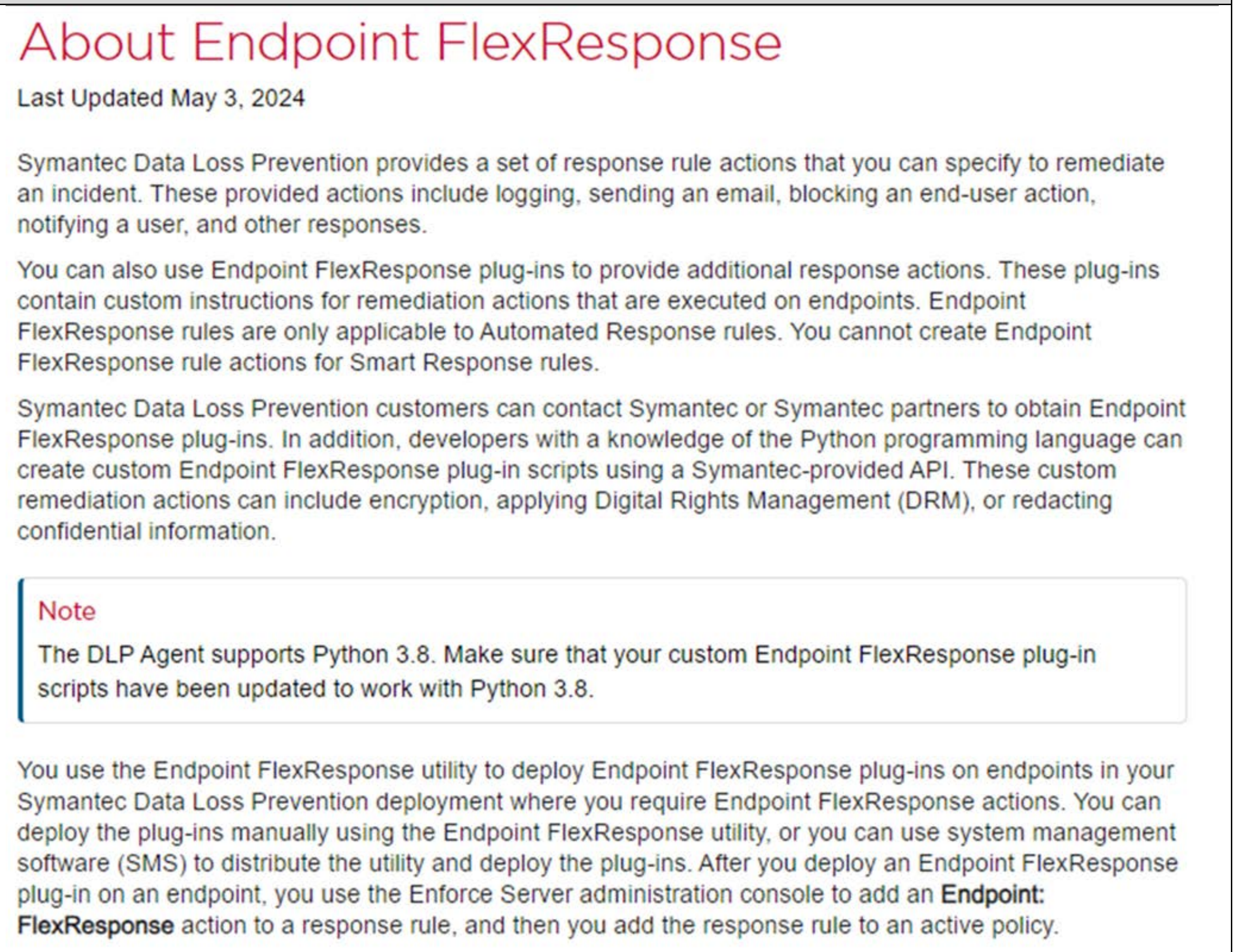
The Symantec CloudSOC Detect app identifies threats based on behavior.

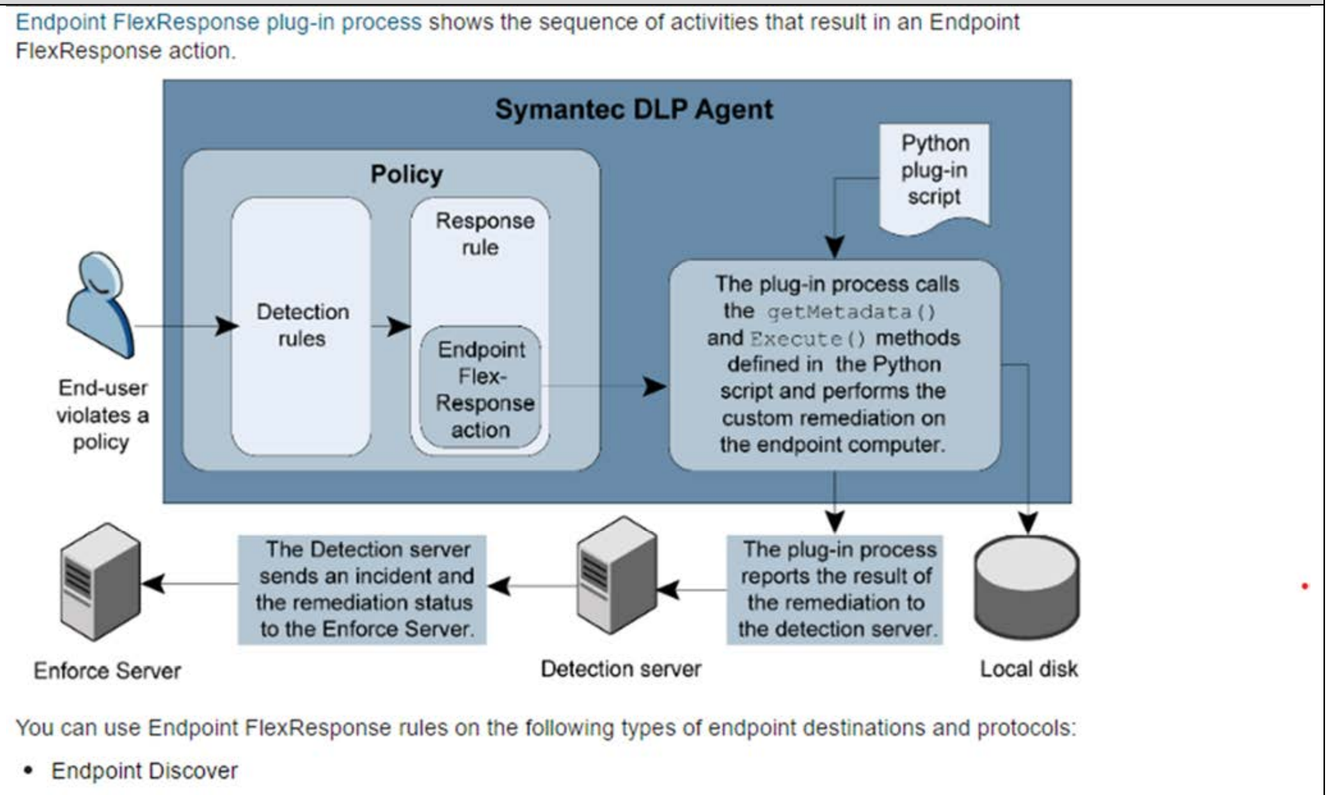
For each Detector, you configure Confidence and Importance levels.

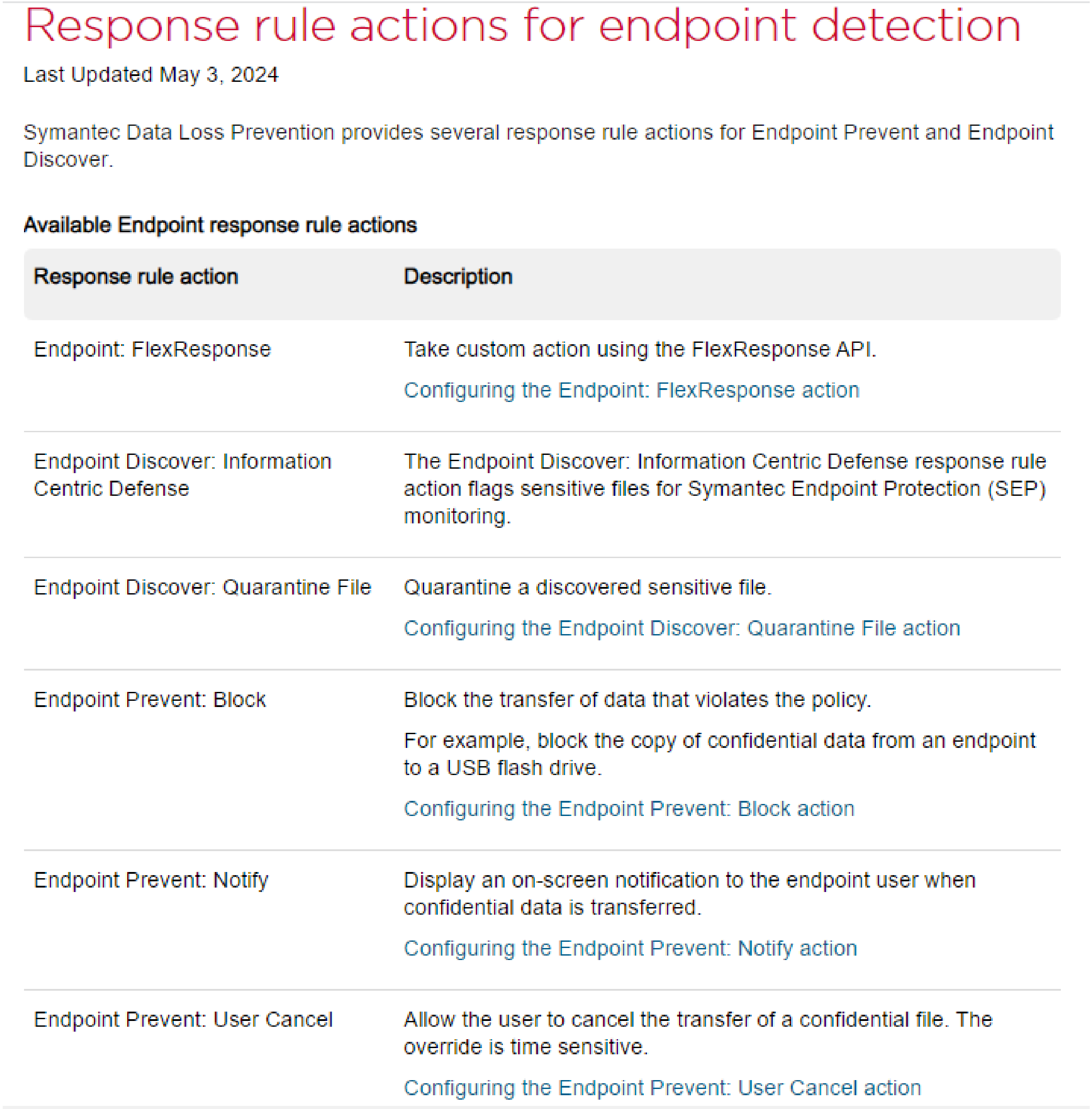
Behavior-based detector	Reports an incident when:
Anomalously large number of user actions	There is an unusually large volume of user actions such as: • Copy • Edit • Open • Preview • Unshare • View instance (for example on AWS) The Detector learns a profile for action volume for each user. It triggers an alert when a user performs a large number of actions uncharacteristic of their historical SaaS app usage.
Anomalously large download data	There is an unusually large amount of data downloaded for a given combination of user and SaaS application. The Detector learns a profile for download volume for each user. It triggers an alert when a user downloads a large volume of data uncharacteristic of their historical SaaS app usage.

Claim 1	Symantec Enterprise Cloud
	 Anomalous variety of file types A user accesses an unusual variety of file types. The Detector learns the number of different types of files that each user interacts with on each individual cloud service. For instance, business analysts might primarily interact with a couple of file types on Google drive. It might be highly unusual if they started interacting with many more file types on Google drive. The learned profile changes over time as the user interacts with different number of file types. The Detector does not evaluate the file's internal content, just the file type extension. To prevent users from getting around this detector, configure the file type mismatch detector to alert you if there are mismatches between the filename extension and true underlying file type. (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/detect-home/understanding-detectors/behavior-based-incident-detectors.html)

<table>
<tr><th>Claim 1</th><th>Symantec Enterprise Cloud</th></tr>
<tr><td>and in response to determining that the electronic file is unauthorized, performing one or more responsive actions.</td><td>
About response rule execution types
Last Updated May 3, 2024
Symantec Data Loss Prevention provides two types of policy response rules: Automated and Smart.
The detection server that reports a policy violation executes Automated Response rules. Users such as incident remediators execute Smart Response rules on demand from the Enforce Server administration console.
Response rule types<table><tr><th>Response rule execution type</th><th>Description</th></tr><tr><td>Automated Response rules</td><td>When a policy violation occurs, the detection server automatically executes response rule actions.
About Automated Response rules</td></tr><tr><td>Smart Response rules</td><td>When a policy violation occurs, an authorized user manually triggers the response rule.
About Smart Response rules</td></tr></table>(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/about-response-rule-execution-types.html)</td></tr>
</table>

Claim 1	Symantec Enterprise Cloud
	 **About Endpoint FlexResponse** Last Updated May 3, 2024 Symantec Data Loss Prevention provides a set of response rule actions that you can specify to remediate an incident. These provided actions include logging, sending an email, blocking an end-user action, notifying a user, and other responses. You can also use Endpoint FlexResponse plug-ins to provide additional response actions. These plug-ins contain custom instructions for remediation actions that are executed on endpoints. Endpoint FlexResponse rules are only applicable to Automated Response rules. You cannot create Endpoint FlexResponse rule actions for Smart Response rules. Symantec Data Loss Prevention customers can contact Symantec or Symantec partners to obtain Endpoint FlexResponse plug-ins. In addition, developers with a knowledge of the Python programming language can create custom Endpoint FlexResponse plug-in scripts using a Symantec-provided API. These custom remediation actions can include encryption, applying Digital Rights Management (DRM), or redacting confidential information. Note The DLP Agent supports Python 3.8. Make sure that your custom Endpoint FlexResponse plug-in scripts have been updated to work with Python 3.8. You use the Endpoint FlexResponse utility to deploy Endpoint FlexResponse plug-ins on endpoints in your Symantec Data Loss Prevention deployment where you require Endpoint FlexResponse actions. You can deploy the plug-ins manually using the Endpoint FlexResponse utility, or you can use system management software (SMS) to distribute the utility and deploy the plug-ins. After you deploy an Endpoint FlexResponse plug-in on an endpoint, you use the Enforce Server administration console to add an **Endpoint: FlexResponse** action to a response rule, and then you add the response rule to an active policy.

Claim 1	Symantec Enterprise Cloud
	 Endpoint FlexResponse plug-in process shows the sequence of activities that result in an Endpoint FlexResponse action. Symantec DLP Agent Policy Detection rules Response rule Endpoint Flex-Response action Python plug-in script The plug-in process calls the getMetadata() and Execute() methods defined in the Python script and performs the custom remediation on the endpoint computer. End-user violates a policy Enforce Server The Detection server sends an incident and the remediation status to the Enforce Server. Detection server The plug-in process reports the result of the remediation to the detection server. Local disk You can use Endpoint FlexResponse rules on the following types of endpoint destinations and protocols: • Endpoint Discover (https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/about-discovering-and-preventing-data-loss-on-endpoints/about-endpoint-flexresponse.html)



Response rule actions for endpoint detection

Last Updated May 3, 2024

Symantec Data Loss Prevention provides several response rule actions for Endpoint Prevent and Endpoint Discover.

Available Endpoint response rule actions

Response rule action	Description
Endpoint: FlexResponse	Take custom action using the FlexResponse API. Configuring the Endpoint: FlexResponse action
Endpoint Discover: Information Centric Defense	The Endpoint Discover: Information Centric Defense response rule action flags sensitive files for Symantec Endpoint Protection (SEP) monitoring.
Endpoint Discover: Quarantine File	Quarantine a discovered sensitive file. Configuring the Endpoint Discover: Quarantine File action
Endpoint Prevent: Block	Block the transfer of data that violates the policy. For example, block the copy of confidential data from an endpoint to a USB flash drive. Configuring the Endpoint Prevent: Block action
Endpoint Prevent: Notify	Display an on-screen notification to the endpoint user when confidential data is transferred. Configuring the Endpoint Prevent: Notify action
Endpoint Prevent: User Cancel	Allow the user to cancel the transfer of a confidential file. The override is time sensitive. Configuring the Endpoint Prevent: User Cancel action

Claim 1	Symantec Enterprise Cloud
	(https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-2/response-rules-2/response-rule-actions-for-endpoint-detection.html)